rectangle dont l'aire m^2n^2 est un carré ; alors $m^2 = u_1^4 - v_1^4$, avec des nombres u_1, v_1, tels que $u_1^2 \pm v_1^2$ soit carré, et on voit que $u_1^2 + v_1^2 < u^2 + v^2$. Cette démonstration donne l'impossibilité de l'équation de Fermat pour l'exposant 4.

Dans sa correspondance ou dans ses travaux publiés, Fermat n'a jamais fait allusion à son équation pour d'autres exposants que 3 et 4. Il est donc permis de penser qu'il s'est aperçu après coup d'une difficulté dans la démonstration qu'il croyait avoir pour le cas général de sa conjecture.

Les successeurs de Fermat

Pendant le XVII^e siècle, l'analyse diophantienne est restée un sujet à la mode qui a intéressé notamment Isaac Newton et Wilhelm von Leibniz. Au premier, on doit une note remarquable dans un cahier de 1670, où il interprète l'équation diophantienne $y^2 = P(x)$, où P est un polynôme de degré égal à trois (de la forme $ax^3 + bx^2 + cx + d$), comme la recherche des points à coordonnées rationnelles sur la courbe définie par cette équation. Newton explique comment une sécante qui joint deux points rationnels (c'est-à-dire dont l'abscisse et l'ordonnée sont des nombres rationnels) recoupe la courbe en un troisième point rationnel, mais cette interprétation par la géométrie algébrique reste isolée, à l'époque *(voir la figure 6)*.

Leibniz avait découvert que certaines manipulations de l'analyse diophantienne conduisant à exprimer rationnellement, en fonction d'un paramètre, des quantités x et y liées par une relation algébrique $f(x,y) = 0$, pouvaient être employées pour obtenir des intégrales de y en fonction de x (l'aire sous la courbe donnée par l'équation $y = f(x)$). On trouve une remarque analogue dans des lettres du mathématicien suisse Daniel Bernoulli (1700-1782) à Christian Goldbach (1690-1764), en décembre 1723 et en mars 1724.

C'est précisément par Goldbach que l'attention du Bâlois Léonard Euler (1707-1783) a été attirée sur les travaux arithmétiques de Fermat, à partir de 1730. Euler a beaucoup étudié le grand théorème de Fermat, et beaucoup de ses travaux sont consacrés à des démonstrations de résultats annoncés par Fermat.

Le premier thème est l'étude des équations diophantiennes de degré égal à deux. En supposant connue une solution rationnelle, il aborde la recherche des autres solutions d'une manière analogue à celle de Diophante pour le problème 8 du livre II, et il remarque que la détermination des solutions entières exige la résolution d'une équation du type de Pell-Fermat.

Un deuxième thème est l'étude des équations de la forme $y^2 = P(x)$, où P est un polynôme de degré égal à trois ou quatre, et des problèmes apparentés. On peut y rattacher l'impossibilité de l'équation $x^4 + y^4 = z^2$, qu'Euler établit, en 1747, par descente infinie, à la manière de Fermat, et dont il tire une série de corollaires.

Les constructions d'Euler relatives à ces équations peuvent s'interpréter géométriquement comme l'avait fait Newton (méthode de la sécante ou de la tangente), mais Euler n'en dit rien. Le lien avec le calcul intégral ne lui avait peut-être pas échappé, car, vers 1780, il transforme l'équation $y^2 = P(x)$ en une autre équation analogue à celle qui donne l'addition des «intégrales elliptiques». Ces intégrales ne s'expriment pas par des fonctions élémentaires (les quatre opérations, l'exponentielle, le logarithme et les fonctions sinus et cosinus) ; elles sont égales aux aires comprises entre l'axe des abscisses et les courbes de la forme $y = R(x, \sqrt{P(x)})$, où R est une fonction rationnelle et où P est un polynôme à une variable de degré trois ou quatre).

Euler a donné une démonstration du théorème de Fermat pour l'exposant égal à 3 ; il y fait une première allusion dans une lettre à Goldbach, en août 1753, puis, en 1759, dans un article consacré aux formes quadratiques $a^2 + 3b^2$ et $m^2 + mn + n^2$: on passe de l'une à l'autre en posant $m = a + b$ et $n = b - a$, et Euler annonce que si t^3 est représenté par la seconde forme, il en est de même de t, ce qui lui permet d'amorcer une démonstration par descente infinie. Il publie une démonstration dans son *Algèbre*, en 1770, où il utilise des nombres complexes de la forme $a + b\sqrt{-3}$ (où a et b sont des nombres entiers), en admettant que ces nombres ont une décomposition en facteurs premiers comme les entiers ordinaires : tout nombre de cette forme se décompose en un produit unique de nombres «premiers» du même type.

Cependant il remarque que l'équation $x^3 + y^3 + z^3 = t^3$ est possible : c'est le problème 16 du livre V de Diophante, qu'il étudie dans un article de 1756. Il pense qu'une somme de trois bicarrés ne peut être un bicarré, tandis qu'une somme de quatre bicarrés peut être un bicarré (l'équation correspondante, $x^4 + y^4 + z^4 + t^4 = u^4$, ne sera résolue qu'en 1911 par le mathématicien américain M. Norrie). Euler croyait encore qu'une somme de quatre puissances cinquièmes ne peut pas être une puissance cinquième, mais, en 1962, M. Birch a trouvé un contre-exemple par ordinateur, démontrant ainsi que cette idée était fausse.

Joseph Louis Lagrange (1736-1813) a pris le relais d'Euler pendant la dizaine d'années où il s'est intéressé à la théorie des nombres. Lagrange obtient d'abord un résultat sur la périodicité des fractions continues de nombres quadratiques : les nombres quadratiques sont les racines d'équations du deuxième degré dont les coefficients sont des nombres entiers (par exemple, $\sqrt{3}$ est un nombre quadratique, parce qu'il est solution de l'équation $x^2 - 3 = 0$). On peut écrire ces nombres sous la forme de fractions continues, de la forme générale $1 + 1/(a_0 + 1/(a_1 + 1/(a_2 + 1/(...))))$; notamment $\sqrt{3}$ s'écrit sous la forme $1 + 1/(1 + 1/(2 + 1/1 + 1/2...))$ dont la périodicité est égale à deux : les 1 et les 2 alternent aux dénominateurs successifs.

À partir de ce résultat, Lagrange établit la possibilité de l'équation de Pell-Fermat dans le cas général. Puis il obtient un critère d'existence d'une solution pour les équations diophantiennes de degré deux (critère qui sera amélioré par Adrien Marie Legendre). Lagrange n'aborde les équations de degré trois ou quatre que dans un article de 1777, où il utilise, sous une forme exclusivement algébrique, la méthode de la tangente.

L'analyse diophantienne au XIX^e siècle

Au XIX^e siècle, de nouveaux cas de la conjecture de Fermat sont progressivement établis : Peter Dirichlet (1805-1859), alors étudiant à Paris, démontre en 1825 l'impossibilité de l'équation $x^5 \pm y^5 = 2^m z^5$, avec m positif, par une descente infinie fondée sur les propriétés des nombres de la forme $a + b\sqrt{5}$. La même année, Legendre démontre le théorème de Fermat pour l'exposant 5. Puis, en 1832, Dirichlet établit le cas de l'exposant 14 au moyen de l'arithmétique des nombres de la

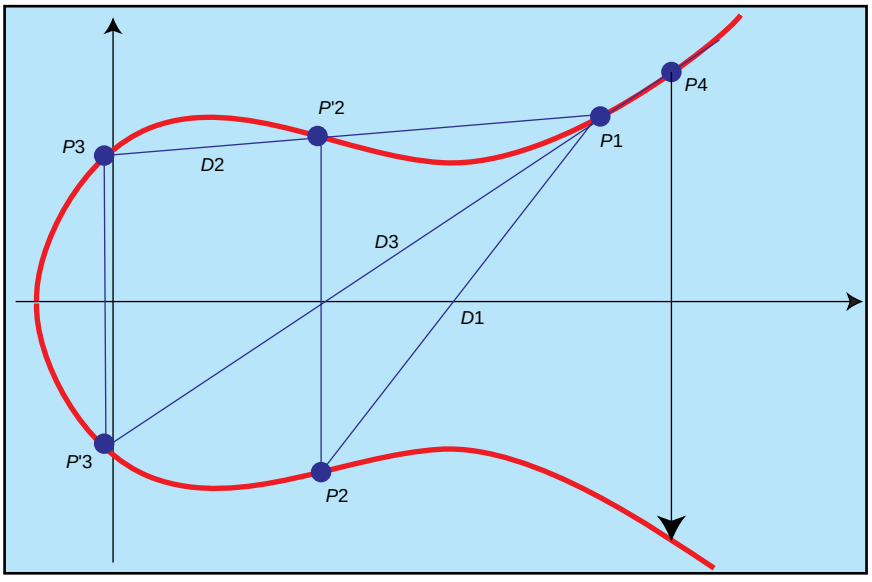
forme $m + n\sqrt{-7}$, où m et n sont nombres entiers, et Gabriel Lamé (1795-1870), en 1839, obtient une démonstration pour l'exposant 7.

Dans les mêmes années, Legendre, Niels Abel (1802-1829) et Sophie Germain (1776-1831) mettent au point des méthodes élémentaires pour atteindre des résultats sur l'impossibilité du premier cas de l'équation de Fermat $x^p + y^p + z^p = 0$, avec p premier impair ne divisant aucun des nombre x, y, z. Sophie Germain démontre que ce cas est impossible s'il existe un nombre premier q tel que p ne soit pas une puissance p-ième modulo q : lorsque $2p + 1$ est premier, par exemple si $p = 11$ ($2p + 1$=23), on peut prendre $q = 2p + 1$ parce que 11 n'est pas une puissance onzième modulo 23 (tout nombre compris entre 1 et 22, élevé à la puissance 11, est un multiple de 23 augmenté ou diminué de 1). Et Legendre étend ce résultat au cas où $4p + 1$ est premier, par exemple si $p = 13$ ($4p + 1$=53).

Le premier travail d'Ernst Kummer (1810-1893), en 1837, sur l'équation de Fermat se rattache au même ordre d'idées ; il établit d'abord que si l'équation $x^{2\lambda} + y^{2\lambda} = z^{2\lambda}$ a une solution telle que λ n'ait pas de facteur commun avec le produit xyz, alors λ a un reste égal à 1 dans la division par 8.

Apparemment Kummer a initialement cru qu'il pourrait démontrer le théorème de Fermat pour un exposant λ premier impair quelconque par une méthode de descente infinie, au moyen de l'«arithmétique des nombres cyclotomiques engendrés par α, une racine λ-ième de 1», envisagée par Gauss dans la septième section de ses *Disquisitiones arithmeticae* : les nombres cyclotomiques sont les nombres de la forme $a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_{\lambda-2}\alpha^{\lambda-2}$, où les nombres a_0, a_1, a_2... $a_{\lambda-2}$ sont des nombres entiers, et où α est une racine λ-ième de l'unité, c'est-à-dire un nombre complexe vérifiant l'équation $x^\lambda = 1$; un tel nombre est représentable par un point du cercle de rayon centré sur l'origine (on peut considérer que l'arc de cercle qui se trouve entre 1 et α est la λ-ième partie de tout le cercle). Si les entiers cyclotomiques avaient admis une décomposition unique en facteurs premiers, une solution (x, y, z) de l'équation de Fermat pour l'exposant λ, sans facteur commun avec x, y et z, aurait conduit à l'égalité :

$$z^\lambda = (x + y)(x + \alpha y)\ldots(x + \alpha^{\lambda-1}y)$$



7. SUITE DE POINTS créée à partir d'une solution ***P*1** de l'équation associée à la courbe en rouge. ***P*1** serait une solution dite «de torsion» si l'une des droites ***D*** était verticale. Les points de torsion forment des groupes dont on a exploré les relations avec les points rationnels.

avec, au second membre, λ nombres sans facteurs communs ; on aurait déduit que ces facteurs devaient être tous des puissances λ-ièmes, ce qui aurait permis d'amorcer une descente infinie.

Toutefois Kummer découvrit en 1844 que l'arithmétique des entiers cyclotomiques était délicate : il n'existe pas toujours de décomposition unique de ces nombres en facteurs cyclotomiques premiers. Pour se raccrocher à l'arithmétique des entiers naturels, Kummer considère la norme des entiers cyclotomiques $f(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_{\lambda-2}\alpha^{\lambda-2}$: cette norme, définie par le produit $f(\alpha)f(\alpha^2)\ldots f(\alpha^{\lambda-1})$, est toujours un nombre entier naturel , et la norme d'un entier cyclotomique premier est un nombre premier ordinaire, de reste égal à 1 dans la division entière par λ

Réciproquement, pour les nombres premiers inférieurs à 1 000, Kummer a laborieusement calculé (à la main, parce qu'il ne disposait alors pas d'ordinateur) des tables de factorisation en entiers cyclotomiques premiers des nombres premiers ordinaires ayant pour reste 1 dans la division entière par λ, pour tous les nombres λ inférieurs à 24. Il a ainsi découvert que, pour λ égal à 23, le nombre premier ordinaire 47 (deux fois 23 plus 1) n'est pas la norme d'un entier cyclotomique, de sorte que les entiers cyclotomiques engendrés par une racine 23-ième de l'unité n'admettent pas de décomposition unique en facteurs premiers. Cela a conduit Kummer à élaborer, dans ses travaux suivants, sa théorie des «nombres premiers idéaux», qu'il ne définissait d'ailleurs pas comme des nombres : il donnait seulement les conditions pour qu'un entier cyclotomique soit divisible par une puissance donnée d'un tel nombre idéal. En termes modernes, les nombres idéaux de Kummer peuvent s'interpréter comme des fonctions associant un nombre entier naturel à chaque entier cyclotomique, avec des conditions particulières ; l'exposant de la puissance du nombre idéal qui divise l'entier cyclotomique est précisément cette fonction.

Kummer définit les produits d'idéaux (on les appellerait aujourd'hui des diviseurs), qu'il groupe en un nombre fini h de classes. En reprenant des idées de Dirichlet, il étudie ce nombre de classes au moyen d'une fonction analogue à la fonction zêta de Riemann (le produit, sur tous les idéaux p premiers, de termes de la forme $1 / (1 - n(p)^{-s})$, où $n(p)$ représente la norme de p). La finitude du nombre de classes permet d'écrire les facteurs $x + \alpha^k y$ de z^λ comme des puissances λ-ièmes multipliées par des facteurs ne pouvant prendre qu'un nombre fini de valeurs. Lorsque λ ne divise pas le nombre de classes, on peut poursuivre la démonstration comme dans le cas où h est égal à 1 (celui de l'arithmétique ordinaire) ; on dit alors que λ est un nombre premier régulier, et Kummer a donné un critère pour reconnaître les nombres