LES ÉQUATIONS DIOPHANTIENNES

Pierre de Fermat (1607 ?-1665) a travaillé sur de nombreuses questions mathématiques, maintenant appartenant à des spécialités différentes, en arithmétique, probabilités, dans le domaine du calcul différentiel. De nombreux thèmes mathématiques peuvent aujourd'hui se réclamer de lui. Nous ne dirons ici que quelques mots sur les questions contemporaines (disons depuis la fin du 19^{e} siècle ou le début du 20^{e}) qui suivent les réflexions de Fermat en arithmétique, plus précisément dans le domaine des "équations diophantiennes".

Diophante d'Alexandrie (3^{e} siècle ?) est un mathématicien grec qui aborda de nombreux sujets arithmétiques. Dans son ouvrage maître, *les Arithmétiques*, il pose très clairement le problème que l'on énonce ainsi aujourd'hui :

Étant donné une équation algébrique à coefficients entiers trouver ses solutions en nombres entiers.

C'est en lisant la traduction latine par Claude Gaspard Bachet de Méziriac (1581-1638) des *Arithmétiques* de Diophante que Fermat transmit à la postérité, par des annotations et des commentaires dans les marges, parmi ses plus belles et parfois énigmatiques idées mathématiques.

Dans la suite nous effleurerons souvent des résultats ou des théories mathématiques en ne donnant que peu de détails et rarement des éléments de bibliographie, mais ceci est facilement corrigé, grâce au réseau, en tapant quelques mots clés.

Pour commencer considérons quelques exemples simples.

$$aX + b = 0 \quad \text{où } a \text{ et } b \text{ sont des entiers, } \quad a \neq 0 \ ,$$

on cherche X ; aujourd'hui on maîtrise le calcul fractionnaire et l'on sait qu'il y a une solution, qui est $X = -\frac{b}{a}$, que c'est une fraction en nombres entiers et que c'est une entier si a divise b.

Exemple $2X - 6 = 0$, alors $X = \dfrac{6}{2} = 3$, $2X + 5 = 0$, alors $X = -\dfrac{5}{2}$,

Date: 15 février 2015.

et cette dernière solution n'est pas un entier. Cette difficulté, de ne pas trouver les solutions voulues pour des équations aussi simples, a été levée en étendant la recherche des solutions des équations diophantiennes aux fractions de nombres entiers ; on parle alors de "solutions rationnelles".

$$aX^2 + bX + c = 0 \quad \text{où } a\ ,\ b \text{ et } c \text{ sont des entiers,} \quad a \neq 0\ ,$$

on sait que si $\Delta = b^2 - 4ac$ est le discriminant de cette équation les solutions sont $X = \frac{-b \pm \sqrt{\Delta}}{2a}$, qu'elles sont donc rationnelles si et seulement si Δ est le carré d'un nombre rationnel (le carré d'une fraction en nombres entiers).

Ce dernier exemple montre qu'il peut y avoir des "solutions" sans qu'elles soient rationnelles. C'est encore plus marquant dans l'exemple d'une équation, cette fois avec deux inconnues X et Y,

$$X^2 + Y^2 = 2$$

qui, si l'on dessine la figure correspondante dans un plan rapporté aux coordonnées (X, Y) est un cercle, contenant donc beaucoup de points, par conséquent l'équation a beaucoup de solutions, mais n'admet que $(X, Y) = (\pm 1, \pm 1)$ pour solutions rationnelles.

L'équation de Pell-Fermat (John Pell, 1611-1685). C'est ainsi qu'elle se nomme aujourd'hui. Elle fut considérée en des temps très anciens, en particulier par Diophante dans ses Arithmétiques. Elle s'écrit en général

$X^2 - aY^2 = b$ où a et b sont des entiers, $a > 0$ et a sans facteur carré.

Nous ne parlerons que du cas $b = \pm 1$, qui est le plus important, même, nous ne considérerons qu'un exemple très concret

(1) $$X^2 - 2Y^2 = \pm 1 \text{ , donc le cas où } \quad a = 2\ .$$

La Théorie algébrique des nombres, création des 19$^{\text{e}}$ siècle et première moitié du 20$^{\text{e}}$, permet maintenant de très bien comprendre cette équation. Nous énonçons le résultat qu'elle permet d'obtenir avant de donner quelques explications. Il existe (au moins) une solution

(2) $$(X_1, Y_1) \quad \text{appelée solution fondamentale}$$

telle que l'ensemble de toutes les solutions s'écrive $(\pm X_n, \pm Y_n)$ où n décrit tous les entiers, où X_n et Y_n sont définis par la relation

$$X_n + Y_n\sqrt{2} = (X_1 + Y_1\sqrt{2})^n \tag{3}$$

Cette résolution de l'équation de Pell-Fermat (avec ± 1 au second membre) provient de l'interprétation qu'en fait la Théorie algébrique des nombres, interprétation qui explique la nature des solutions ([1]).

La Théorie algébrique des nombres consiste en une généralisation de $\mathbb{Q}$, le corps des fractions en nombres entiers, de son sous-anneau $\mathbb{Z}$ des entiers et de la factorisation de tout entier positif en un produit de nombres premiers, uniques à permutations près.

Pour l'équation étudiée (1) nous considérons le corps $\mathbb{Q}[\sqrt{2}]$ formé par les nombres de la forme $u = r + s\sqrt{2}$, où r et s sont des éléments de $\mathbb{Q}$, son sous-anneau $\mathbb{Z}[\sqrt{2}]$ où cette fois r et s sont des entiers. Quant à l'analogue de la factorisation en nombres premiers nous n'en dirons rien (c'est la notion d'anneau factoriel, que l'on ne rencontre que rarement, ou celle d'anneau de Dedekind).

On note $(\mathbb{Z}[\sqrt{2}])^\times$ le groupe des éléments inversibles (pour la multiplication) de l'anneau $\mathbb{Z}[\sqrt{2}]$, c'est à dire des éléments $u = r + s\sqrt{2}$ avec r et s entiers (et non tous deux nuls) tels que

$$\frac{1}{u} = \frac{1}{r + s\sqrt{2}} = \frac{r}{r^2 - 2s^2} + \frac{s}{r^2 - 2s^2}\sqrt{2}$$

soit aussi dans $\mathbb{Z}[\sqrt{2}]$. Il faut remarquer que si $r+s\sqrt{2}$ est dans $(\mathbb{Z}[\sqrt{2}])^\times$ il en est de même de $r - s\sqrt{2}$, donc aussi de leur produit

$$(r + s\sqrt{2})(r - s\sqrt{2}) = r^2 - 2s^2 \ ,$$

mais r^2-2s^2 est un entier, qui est donc inversible pour la multiplication, par suite égal à ± 1.

On vient de montrer que si $r + s\sqrt{2}$ est dans $(\mathbb{Z}[\sqrt{2}])^\times$ alors r et s sont solutions de l'équation de Pell-Fermat (1). La réciproque se montre facilement et ceci est en fait une équivalence.

Un théorème important de Dirichlet (Johann Peter Gustav Lejeune Dirichlet, 1805-1859), appelé le "Théorème des unités", montre que le groupe multiplicatif $(\mathbb{Z}[\sqrt{2}])^\times$ est *de rang* 1, ce qui veut dire ici qu'il existe un élément u_1 de ce groupe tel que pour tout autre élément u il

1. Pour beaucoup des notions qui vont plus ou moins apparaître dans la suite nous renvoyons aux différents ouvrages de J.S. Milne <http ://www.jmilne.org/math/>.

existe un unique entier n (positif, négatif ou nul) tel que l'on ait

$$u = \begin{cases} u_1^n \\ \text{ou bien} \\ -u_1^n \end{cases}$$

Ainsi se trouve expliquée la forme des solutions (3) de l'équation de Pell-Fermat (1). Il faut cependant remarquer qu'il reste à déterminer u_1, c'est à dire X_1 et Y_1, cf (2).

On utilise alors l'algorithme des fractions continues, qui permet de calculer les meilleures approximations rationnelles des nombres irrationnels([2]). Cet algorithme appliqué à $\sqrt{2}$ donne

$$u_1 = 1 + \sqrt{2} \quad \text{donc} \quad X_1 = 1 \text{ et } Y_1 = 1 \ ,$$

et les solutions (X_n, Y_n) de l'équation de Pell-fermat (1) sont données par la relation

$$X_n + Y_n\sqrt{2} = (1 + \sqrt{2})^n \ ,$$

où n est un entier positif, négatif ou nul.

Un exemple de courbe elliptique : $Y^2 = X^3 - 2$.

Il existe de nombreuses courbes elliptiques, dans une situation suffisamment générale elles s'écrivent sous la forme

$$Y^2 = aX^3 + bX^2 + cX + d \tag{4}$$

où a, b, c, et d sont des constantes, par exemple des nombres rationnels. Ce sont des courbes complètes (c'est à dire qu'il ne leur manque pas de point), régulières (c'est à dire que leurs dessins n'ont pas d'angle vif). Ce sont les courbes de genre 1 : le genre d'une courbe est un nombre qui en traduit la complexité, une sorte d'évaluation de la différence entre la courbe et ses tangentes, c'est-à-dire entre elle et une droite ; une droite est en effet de genre 0 ; on dira un mot plus bas des courbes de genre ≥ 2. Les courbes elliptiques ont une propriété étonnante et qui les caractérisent : leurs points forment un groupe, c'est-à-dire que l'on peut "additionner" leurs points, les "retrancher"...

On s'intéresse aux courbes d'équations de la forme (4) et telles que a, b, c, et d soient rationnels, c'est à dire des fractions en nombres entiers. Ce sont alors des équations diophantiennes et rechercher leurs points (X, Y) avec X et Y rationnels (les points rationnels) est résoudre ces équations. Un théorème célèbre de Louis Mordell (1888-1972) et d'André Weil (1906-1998) dit qu'il existe un entier $n \geq 0$ et des points rationnels $P_1 \cdots P_n$ tels qu'en les ajoutant, retranchant de toutes les

2. on peut trouver l'algorithme des fractions continues dans tous les ouvrages qui traitent de l'approximation des nombres réels par des nombres rationnels

manières, c'est à dire en considérant le groupe ainsi engendré, on obtienne l'ensemble des points rationnels, ou plus exactement, si l'on suppose qu'il n'y a pas de relation entre ces points $P_1 \cdots P_n$, pour les avoir tous en plus du groupe engendré il faut encore ajouter un ensemble fini de points. L'ensemble des points rationnels est un groupe (pour la même opération que celles existant sur tous les points), il est appelé le groupe de Mordell-Weil de la courbe et l'entier n (lorsqu'il n'y a pas de relation entre les points $P_1 \cdots P_n$) est le rang de Mordell-Weil (et le cas $n = 0$ signifie simplement que ces P_i, sans relation, n'existent pas, que le groupe de Mordell-Weil est fini).

En général on ne sait pas calculer le rang de Mordell-Weil d'une courbe elliptique. Beaucoup d'informations sont proposées par une conjecture célèbre, datant du début des années soixante et due à Bryan John Birch (1931-) et à Sir Henry Peter Francis Swinnerton-Dyer (1927-), mais dont il semble que l'on soit bien loin de pouvoir y répondre.

Revenons à la courbe elliptique $Y^2 = X^3 - 2$. On sait en déterminer son groupe de Mordell-Weil et une curieuse propriété en résulte.

On écrit cette équation plutôt sous la forme

$$X^3 = Y^2 + 2$$

et l'idée vient alors de l'étudier dans l'anneau $\mathbb{Z}[i\sqrt{2}]$ dont les éléments sont les $u + vi\sqrt{2}$ où u et v sont des entiers et i vérifie $i^2 = -1$, par suite $(i\sqrt{2})^2 = -2$ ([3]). C'est un anneau qui ressemble à celui envisagé lors de l'équation de Pell-Fermat, mais ici $i\sqrt{2}$ est à la lace de $\sqrt{2}$. Cet anneau se comporte comme celui $\mathbb{Z}$ des entiers, on a

$$X^3 = Y^2 + 2 = (y - i\sqrt{2})(y + i\sqrt{2})$$

et en faisant des raisonnements arithmétiques comparables à ceux plus usuels entre les entiers il vient que les seules solutions en nombres entiers de cette dernière équation sont $(X, Y) = (3, \pm 5)$. Cette équation peut aussi s'écrire $Y^2 + 1 = X^3 - 1$, la solution $(X, Y) = (3, 5)$ nous dit évidement que $5^2 + 1 = 3^3 - 1$, mais aves les raisonnements précédents beaucoup plus, elle donne la réponse à une question que Fermat s'était posé, celle de trouver les entiers précédés par un cube et suivis par un carré : on a $5^2 + 1 = 3^3 - 1 = 26$, donc

Il existe un unique entier précédé par un carré et suivi par un cube, c'est 26.

---

3. i n'est donc pas un nombre usuel puisque son carré est négatif, la nécessité de considérer de tels nombres est apparue au 17^{e}siècle dans l'étude des polynômes de degré 3 ; i est bien connu des électriciens, qui l'appellent j, pour ne pas le confondre avec l'intensité.

Les courbes de genre au moins 2. Vers 1921/1922 Mordell conjectura que les courbes de genre au moins deux et définies sur les nombres rationnels n'ont qu'un nombre fini de points rationnels, c'est à dire qu'un système fini d'équations dont les coefficients sont des fractions d'entiers, donc un système fini d'équations diophantiennes, dont les inconnues sont X, Y, Z, ..., qui définit une courbe de genre plus grand ou égal à 2, n'admet qu'un nombre fini de solutions $(X, Y, Z, \cdots)$ où X, Y, Z, ... sont des fractions d'entiers. Cette conjecture fut démontrée par Gerd Faltings (1954-) en 1983.

Prenons l'exemple de "l'équation de Fermat"

$$X^n + Y^n = Z^n \ . \tag{5}$$

Pour $n = 3$ c'est une courbe elliptique. Montrons ceci. L'équation (5) peut s'écrire

$$Z^3 - X^3 = Y^3 \text{ donc } \left(\frac{Z}{Y}\right)^3 - \left(\frac{X}{Y}\right)^3 = 1 \text{ ou encore}$$

$$\left(\frac{Z}{Y} - \frac{X}{Y}\right)\left(\left(\frac{Z}{Y}\right)^2 + \frac{Z}{Y}\frac{X}{Y} + \left(\frac{X}{Y}\right)^2\right) = 1$$

il est alors naturel de choisir comme nouvelle inconnue la première parenthèse, de poser $U = \frac{Z}{Y} - \frac{X}{Y}$, et de le faire apparaître dans la deuxième parenthèse. Il vient

$$U\left(\left(U + \frac{X}{Y}\right)^2 + \left(U + \frac{X}{Y}\right)\frac{X}{Y} + \left(\frac{X}{Y}\right)^2\right) = 1$$

ou encore

$$U^3\left(\left(1 + \frac{X}{YU}\right)^2 + \left(1 + \frac{X}{YU}\right)\frac{X}{YU} + \left(\frac{X}{YU}\right)^2\right) = 1$$

et en arrangeant la parenthèse

$$U^3\left(3\left(\frac{X}{YU}\right)^2 + 3\left(\frac{X}{YU}\right) + 1\right) = 1 \ ,$$

finalement, en posant $T = \frac{1}{U}$ et $S = \frac{X}{YU}$ il vient

$$T^3 = 3S^2 + 3S + 1 \ , \tag{6}$$

qui est bien l'équation d'une courbe elliptique, cf (4) ; il faut remarquer que tous les changements de variables utilisent des formules qui conservent les nombres rationnels, donc transforment des solutions rationnelles de cette dernière équation en des solutions rationnelles de l'équation de Fermat pour $n = 3$. Comme l'on sait depuis le 18$^{\text{e}}$ siècle que cette dernière n'a pas de solutions en nombres entiers et même

rationnels, la relation (6) définit une courbe elliptique sans points rationnels, son rang de Mordell-Weil est 0.

Pour $n \geq 4$ l'équation de Fermat (5) définit une courbe de genre ≥ 2, donc le théorème de Faltings nous dit depuis 1983 que l'équation de Fermat (5) pour $n \geq 3$ n'a qu'un nombre fini de solutions rationnelles. Mais le théorème de Faltings ne donne pas une borne explicite du nombre de ces solutions et il n'est pas possible d'en déduire le "Théorème de Fermat", qui demande que l'équation (5) n'ait aucune solution rationnelle. La recherche de bornes explicites pour le nombre de solutions rationnelles des équations diophantiennes a donné lieu à la création d'une nouvelle théorie appelée du nom de son initiateur la théorie d'Arakelov (Suren Arakelov, 1947-).

Mais c'est Andrew Wiles (1953-) qui en 1994 donna une démonstration du "Théorème de Fermat", avec des méthodes assez différentes de celles qui viennent d'être abordées et dont nous disons quelques mots dans l'un des paragraphes suivants, celui sur le programme de Langlands.

La théorie de Galois. Durant sa courte vie Évariste Galois (1811-1832) pressentit que la compréhension des équations diophantiennes données par les polynômes d'une variable, c'est à dire de la forme

$$P(x) = a_0 + a_1 X + a_2 x^2 + \cdots + a_i X^i + \cdots + a_d X^d \ , \tag{7}$$

où les coefficients a_i sont des nombres rationnels, viendrait de celle des permutations de leurs racines qui laissent invariable le polynôme([4]). Avant d'examiner quelques exemples précisons ce que veut dire le mot "racine". Il s'agit d'un "nombre" qui annule le polynôme, par exemple le polynôme $X^2 + 1$ a pour racine le nombre i que nous avons déjà rencontré, qui vérifie $i^2 = -1$, donc qui n'est pas un nombre usuel : il existe un lieu, contenant tous les nombres réels mais un peu plus gros, appelé le corps des nombres complexes (et il possède des opérations qui prolongent celles entre les nombres réels) dans lequel tous les polynômes (7) ont toutes leurs racines.

Venons-en aux exemples.
Le polynôme X^2+1 a pour racines i et $-i$, les permuter ne change pas le polynôme.
Soit le polynôme $X^3 + pX + q$ (où p et q sont des nombres rationnels),

4. Il existe de nombreux ouvrages sur la théorie de Galois, parfois intitulés Extension de corps, ou Théorie des corps..., par exemple
< http ://www.math.univ-toulouse.fr/ reversat/pedagogie.html >.

on désigne par x_1, x_2 et x_3 ses racines et on pose

$$\Delta = ((x_1 - x_2)(x_2 - x_3)(x_3 - x_1))^2 \ ,$$

c'est le discriminant du polynôme, on peut vérifier alors par le calcul que

$$\Delta = -4p^3 - 27q^2 \ .$$

Supposons que ce discriminant Δ soit le carré d'un nombre rationnel, c'est à dire qu'il existe un nombre rationnel δ tel que

$$\delta = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1), \quad \text{donc} \quad \delta^2 = \Delta \ ,$$

alors les permutations des racines préservant le polynôme doivent laisser δ invariant ; il n'y a que 6 permutations de l'ensemble à 3 éléments $\{x_1, x_2, x_3\}$ et l'on voit qu'il n'y en a que 3 qui préservent δ : la permutation qui décale les indices de 1, c'est à dire qui envoie x_1 sur x_2, x_2 sur x_3 et x_3 sur x_1, cette permutation appliquée deux fois (donc qui décale les indices de 2) et l'identité qui ne bouge rien. Par exemple la permutation qui échange x_1 et x_2 et qui laisse x_3 fixe change δ en $-\delta$. Quand Δ n'est pas le carré d'un nombre rationnel alors toutes les permutations possibles des racines conviennent, il y en 6.
Par exemple, les permutations des racines qui laissent $X^3 + X + 1$ invariant sont au nombre de 6, mais il n'y en a que 3 pour $X^3 - 3X + 1$.

Pour résumer la théorie de Galois (très) brièvement, comme il vient d'être dit, elle consiste à remplacer l'étude des équations polynomiales par celles des permutations de leurs racines qui laissent le polynôme invariant, ces permutations forment un groupe (on peut les composer, c'est à dire appliquer les permutations successivement aux racines), appelé le *groupe de Galois* du polynôme. Ce point de vue avait été envisagé avant Galois, en particulier par Leonhard Euler (1707-1783), mais Galois en a deviné tout l'intérêt.

La théorie de Galois est maintenant bien comprise, elle a été parfaitement mise au point par Emil Artin (1898-1962) et publiée à University Notre Dame Press (Indiana, USA) en 1942, où Artin, professeur à Hambourg, s'était réfugié après avoir fui le nazisme.

La théorie de Galois, si elle est bien comprise, n'en garde pas moins quelques mystères, surtout si l'on se pose par exemple la question de savoir parmi tous les types de groupes qui existent quels sont ceux qui sont des groupes de Galois sur les nombres rationnels ? Autrement dit, puisque cette théorie dit qu'il existe un gros groupe contenant les groupes de Galois de tous les polynômes à coefficients rationnels, appelé le groupe de Galois absolu sur les nombres rationnels, que l'on va noter $\mathcal{G}$, la question est : comment décrire ce groupe $\mathcal{G}$?

Nous ne disons que quelques mots des deux projets principaux cherchant à répondre à cette question, et qui sont en plein débat aujourd'hui.

Le programme de Langlands. Proposé par Robert P. Langlands (1936-) dans une lettre à André Weil en 1967 et fortement développé depuis, en particulier par son initiateur, même si c'est l'un des grands chantiers de ce début du 21^{e} siècle. Suivant en cela d'importants travaux en théorie des nombres de Dirichlet, Hecke (Erich Hecke, 1881-1947) et d'Artin, Langlands propose des espaces (les espaces de formes automorphes) où des groupes agissent et permettent de décrire les actions du groupe $\mathcal{G}$. Ce programme est très largement ouvert aujourd'hui et loin de ses aboutissements, même si la démonstration du Théorème de Fermat s'y insère. De plus, il a un analogue dans un domaine voisin dont nous n'avons rien dit dans cette note, l'arithmétique en caractéristique positive, où il a notablement progressé en 1999/2000, par des travaux dus à Laurent Lafforgue (1966-), puis en 2012 par Vincent Lafforgue (1974-).

Les dessins d'enfants. C'est le nom que donne Alexandre Grothendick (1928-2014) au programme qu'il propose pour déterminer le groupe de Galois $\mathcal{G}$. Ses idées sont décrites en particulier dans son texte "Esquisse d'un programme" (que l'on peut trouver sur le réseau). On en dit quelques mots. Étant donné un polynôme comme (7), à coefficients rationnels, on lui ajoute une variable et il devient l'équation d'une courbe algébrique, définie sur les nombres rationnels. Un théorème de Belyi (Gennadil Vladimirovich Belyi, 1951-2001) datant de la fin des années soixante-dix, dit que de telles courbes peuvent être interprétées comme des "revêtements de la droite ramifiés en trois points". Pour comprendre cette dernière expression considérons l'image d'une bande de pâte à tarte tombant doucement en accordéon sur un chou de pâtissier, quelques soufflets -mais pas tous- de cet accordéon s'écrasent en trois points, ce sont les points de ramification. Un tel revêtement possède un groupe, celui qui agit sur le revêtement sans le changer globalement, donc en ne modifiant pas l'ensemble des points de ramification (mais ils peuvent être échangés entre eux). Les permutations du revêtement agissent sur un ensemble fini, celui des points de ramification, on peut joindre ces points par des arêtes traduisant les échanges, cela donne des sortes de dessins, que Grothendieck a qualifiés d'enfants. En reprenant et améliorant les idées de divers auteurs, dont David Hilbert

(1862-1943), Grothendieck avance que les groupes de Galois des polynômes (7) sont réalisés par ces groupes de revêtements. Cette théorie est encore très largement ouverte.

Merci lecteur d'être arrivé au bout de ce texte, sans aucun doute parfois sibyllin. Il traite de sujets complexes, dont l'élaboration a demandé plusieurs générations d'efforts, parfois des siècles et ce n'est pas simple de le raconter . La mathématique n'est pas une science figée, au contraire de ce que l'on peut parfois ressentir à la lecture des manuels scolaires, elle est en plein mouvement dans de nombreux domaines, nous avons essayé de le montrer en considérant quelques questions d'arithmétique.

Marc Reversat, Institut de Mathématiques de Toulouse.