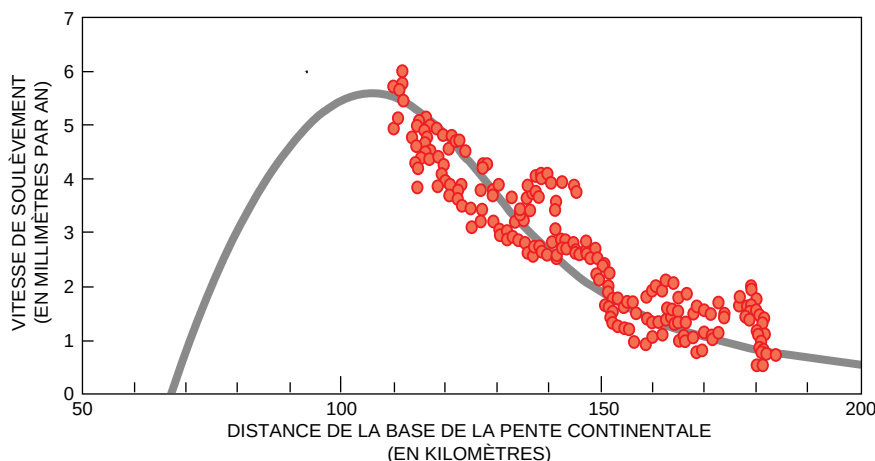


température en fonction de la profondeur. Près de la surface, les sédiments argileux qui tapissent le plancher océanique lubrifient la partie de la faille proche de l'océan. Cependant, plus profondément, les argiles se transforment en des minéraux plus durs, qui empêchent la faille de glisser. Ces changements minéralogiques se produisent à une profondeur de dix kilomètres environ, c'est-à-dire lorsque la température atteint 150 degrés.

L'augmentation de température détermine également la position de la partie profonde de la zone bloquée vers le continent. Aux températures modérées, les roches ont des comportements de frottement normaux : la très forte résistance au mouvement chute lorsque la faille commence à bouger. Ainsi, une fois le glissement commencé, le mécanisme s'emballé, libérant l'énergie élastique et causant un séisme. En revanche, plus en profondeur, dans la croûte, lorsque la température est supérieure à 350 degrés, les roches en contact sur les bords de la faille se comportent comme des fluides visqueux : plus les mouvements sont rapides, plus la résistance est forte. Les parties les plus profondes et les plus chaudes de la faille peuvent alors se déformer par fluage sans engendrer d'ondes élastiques.

Ces températures correspondent-elles aux véritables limites de la zone bloquée? Nous avons étudié cette question en modélisant numériquement les températures sur la faille de la zone de subduction. Les résultats ont confirmé que la profondeur à laquelle la roche atteint une température de 350 degrés correspond bien à la limite profonde de la zone bloquée déterminée par les mesures de déformation.

Une question demeure néanmoins : la zone que nous avons modélisée correspond-elle réellement à la région source des grands tremblements de terre? Nous le pensons, car le déplacement vertical que notre modèle prédit pour une rupture de la zone bloquée rend bien compte des observations des dépôts côtiers enfouis. Des indications supplémentaires nous encouragent à appliquer notre méthode à d'autres zones de subduction. Avec mes collègues Kelin Wang et Makoto Yamano, de l'Université de Tokyo, j'ai montré que la largeur de la zone bloquée de la marge Nankai, au Sud-Ouest du Japon, correspond à la surface de rupture du séisme de magnitude huit qui a frappé cette région en 1940. Par analogie, nous



6. LES NIVELLEMENTS successifs de la côte de la région des Cascades montrent son soulèvement (les points rouges). Les calculs (la courbe grise) rendent bien compte des observations pour la déformation de la plaque Nord-américaine ; ils servent à localiser la partie bloquée de la faille de subduction.

pouvons prévoir le séisme qui frappera la côte Nord-américaine.

Le jour de la catastrophe

Quelle pourrait être l'intensité du mouvement du sol pour les villes de la côte Ouest pendant un grand séisme? Tout dépend de la magnitude du séisme et de la position de son foyer. La magnitude maximale, tout d'abord, dépend de la distance de la côte au lieu de libération de l'énergie sismique. Si l'on se fonde sur les études de séismes déjà analysés, une rupture de toute la faille, de la Colombie britannique jusqu'à la Californie, serait surprenante. Toutefois, si la totalité de la zone bloquée (une surface de près de 100 000 kilomètres carrés) lâchait d'un coup, le séisme pourrait avoir une magnitude égale à neuf, et les dégâts seraient bien pires que ceux du séisme de San Francisco en 1906. Seulement deux événements de cette taille ont été enregistrés à ce jour : un tremblement de terre le long des côtes du Chili, en 1960, et un autre en Alaska, en 1964.

Il existe deux manières d'estimer le mouvement du sol qui résulterait d'un tel séisme. La première consiste à comparer les situations le long de la côte Ouest de l'Amérique du Nord avec ce qui s'est passé ailleurs. La seconde revient à utiliser des modèles de rupture élastique et de déplacements de failles. La conclusion des deux approches est semblable : le prochain grand séisme dans la région des Cascades engendrera des ondes sismiques destructrices qui dureront plusieurs minutes ; puis, lorsque les secousses cesseront, la plupart des régions

côtières se seront enfoncées de un à deux mètres et auront été déplacées de près de dix mètres vers la mer.

Heureusement, la partie bloquée de la faille qui engendrerait un tel tremblement de terre est située principalement sous le plateau continental et ne s'étend que peu sous la côte. Ainsi, Vancouver, Seattle et Portland (qui sont entre 100 et 200 kilomètres à l'intérieur des terres) sont moins exposées aux secousses que les sites proches de la côte Ouest ; elles restent toutefois menacées, car l'énergie sismique se propage à des distances considérables. Plus généralement, les Américains et les Canadiens de la côte Pacifique qui pensaient vivre sur un sol tranquille doivent accepter d'être sous la menace permanente d'un tremblement de terre destructeur.

Roy HYNDMAN est chercheur au Centre de géosciences du Pacifique du Service géologique canadien.

A. NELSON et al., *Radiocarbon Evidence for Extensive Plate-Boundary Rupture about 300 Years ago at the Cascadia Subduction Zone* in *Nature*, vol. 378, pp. 371-374, 23 novembre 1995.

Garry C. ROGERS, *Seismic Potential of the Cascadia Subduction Zone*, in *Nature*, vol. 332, p. 17, 3 mars 1988.

Thomas H. HEATON, *Cascadia Subduction Zone : The Calm before the Quake?*, in *Nature*, vol. 343, pp. 511-512, 8 février 1990.

R.B. HYNDMAN et K. WANG, *Thermal Constraints on the Zone of Major Thrust Earthquake Failure : The Cascadia Subduction Zone*, in *Journal of Geophysical Research (Solid Earth)*, vol. 98, n° 2, pp. 2039-2060, 10 février 1993.

Fermat enfin démontré

YVES HELLEGOUARCH

La démonstration du théorème de Fermat par Andrew Wiles s'appuie sur un faisceau de méthodes mathématiques qui bouleverse le paysage de la théorie des nombres.

Vers la fin de sa vie, Pierre de Fermat (1601-1665), écrivait, dans ses *Défis aux mathématiciens* : «On sait qu'Archimède n'a pas dédaigné de travailler sur des propositions de Conon, qui étaient vraies, mais non prouvées, et qu'il a su les munir de démonstrations d'une haute subtilité. Pourquoi n'espérerais-je pas un semblable secours de vos éminents correspondants, pourquoi, Conon français, ne trouverais-je pas des Archimède anglais?»

Le 23 juin 1993, plus de 300 ans après la note marginale de Fermat, Andrew Wiles, professeur à Princeton (États-Unis), mais fils d'un professeur de théologie anglais, pensait pouvoir annoncer à l'Institut Newton, à Cambridge (Grande-Bretagne) qu'une des propositions que Fermat nous avait léguées – peut-être involontairement, car on peut se demander si la remarque qu'il avait faite en marge d'un exemplaire des *Arithmétiques* de Diophante était destinée à être publiée – était désormais munie d'une démonstration d'une haute subtilité et d'une éblouissante beauté. Il semblait que Fermat avait trouvé son Archimède anglais.

Pourtant, un des artifices d'Andrew Wiles était encore en porte-à-faux, et ce n'est que le 19 septembre 1994, à l'issue d'un labeur intense et grâce au renfort de son collègue Richard Taylor de l'Université de Cambridge, que la magnifique cathédrale édiflée par A. Wiles était enfin libérée de tout échafaudage et s'élevait triomphante dans le ciel mathématique, symbole d'un labeur de trois siècles (ce qui n'est pas exceptionnellement long pour une cathédrale). Cette dernière hésitation du destin illustre bien les mystères et les surprises recelées par le «dernier théorème de Fermat».

Position du problème

L'article de Christian Houzel du mois dernier nous a rappelé l'Histoire de la recherche des triplets pythagoriciens, les entiers x, y et z , solutions en nombres entiers de l'équation $x^2 + y^2 = z^2$ (1). Ces triplets pythagoriciens sont en correspondance avec les points du cercle centré sur l'origine, de rayon unité et d'équation $u^2 + v^2 = 1$, points dont les deux coordonnées sont rationnelles, c'est-à-dire de la forme a/b où a et b sont entiers. Il suffit, pour s'en convaincre, de diviser les deux membres de l'équation (1) par z^2 .

La résolution de cette équation (1), dite diophantienne, est connue depuis fort longtemps. Pour les exposants supérieurs à 2, les équations de la forme $x^n + y^n = z^n$, la solution est radicalement différente. L'assertion de Fermat est que, pour les valeurs de l'exposant n supérieures à 2, les seules solutions entières sont «triviales» : l'un des trois nombres entiers est nul (par exemple, $x = 0$ et $y = z$), ce que l'on exprime en notant que le produit xyz est alors égal à zéro.

Revenons à l'interprétation géométrique : les courbes représentant l'équation $u^n + v^n = 1$ appartiennent à deux familles : une première famille où l'exposant est pair (n est égal à $2p$), et la seconde où l'exposant est impair (n est égal à $2p + 1$). Le cas n égal à 4 a été résolu par Fermat lui-même. Le cas où n est égal à $2p$ avec p impair résulte du cas où n est impair. En effet, en posant $u' = u^2$ et $v' = v^2$ et en remplaçant dans l'équation, on voit qu'il ne reste plus qu'à traiter le cas impair.

On peut même se limiter au cas où n est premier (et évidemment différent de 2), bien que la spécification que le nombre p doit être premier semble très restrictive. En fait cette limi-

tation de la portée du théorème est trompeuse : si l'équation de Fermat pour le nombre p premier n'a pas de solution, alors comme $(x)^{kp}$ est égal à $(x^k)^p$ la solution n'existe pour aucun multiple de p .

Dans le cas où p est premier impair, la courbe $u^p + v^p = 1$ possède trois points rationnels triviaux, le point $(u,v) = (1,0)$, le point $(u,v) = (0,1)$, et le point à l'infini de la courbe, lequel correspond à la solution $(x,y,z) = (1,-1,0)$ de l'équation diophantienne $x^p + y^p = z^p$. L'assertion de Fermat revient à dire que si p est premier et différent de 2, la courbe $u^p + v^p = 1$ n'admet pas d'autre point rationnel : il faut démontrer qu'il n'y a que trois points rationnels sur la courbe.

Les derniers résultats classiques

Lorsqu'ils sont bloqués dans leurs recherches, les mathématiciens ont une stratégie particulière : ils étudient des variations du problème qu'ils présentent sous des formes différentes. Le grand mathématicien Niels Henrik Abel écrivait que l'on devait donner à un problème d'impossibilité «une forme telle qu'il soit toujours possible de le résoudre, ce que l'on peut toujours faire... Au lieu de demander une relation dont on ne sait pas si elle existe ou non, il faut (se) demander si une telle relation est en effet possible». On en déduit alors les limites de possibilité du problème original.

C'est ainsi que les algébristes italiens du XVI^e siècle ont introduits les nombres «imaginaires» pour étudier les solutions réelles des équations algébriques. Pragmatique, Newton écrivait : «il faut bien que dans les équations, il y ait des racines impossibles (entendez «imaginaires») sans quoi, dans les problèmes (physiques), cer-

tains cas impossibles se trouveraient possibles».

En théorie des nombres, les mathématiciens varient la structure : au lieu d'examiner les solutions entières des équations, ils examinent les solutions modulo k . Ils regroupent dans une même classe les nombres qui ont le même reste après division par k . Ainsi la classe des nombres pairs est constituée par les nombres égaux à zéro modulo 2.

Les entiers modulo k ont une structure d'anneau, c'est-à-dire qu'ils sont munis d'une addition et d'une multiplication reflétant l'addition et la multiplication ordinaires. Lorsque k est égal à 2 les restes sont 0 et 1, et l'on a :

+	0	1
0	0	1
1	1	0
ADDITION		

×	0	1
0	0	0
1	0	1
MULTIPLICATION		

En utilisant la loi de réciprocité quadratique due à Euler, Legendre et Gauss, le mathématicien Gérard Terjanian a su faire resplendir, en 1977, les méthodes traditionnelles d'un éclat particulier.

Il a démontré que, si n est égal à $2p$, où p est un nombre premier impair, alors l'un des trois nombres x, y, z vérifiant l'équation de Fermat pour l'exposant $2p$, est égal à zéro modulo $2p$, c'est-à-dire est divisible par n . C'était la première fois qu'un résultat aussi général était obtenu pour ce qu'il est convenu d'appeler le «premier cas du théorème de Fermat».

Dans les méthodes classiques, mais pas dans la méthode de A. Wiles, la démonstration de Fermat comporte toujours deux étapes. La première, que l'on appelle le «premier cas» est la plus facile ; elle consiste à démontrer, lorsque l'exposant est un nombre premier p , que p divise l'un des trois nombres x, y, z vérifiant l'équation de Fermat.

Donnons un exemple d'une telle démonstration. Par exemple, si p est égal à 3, on examine les solutions modulo 9 de l'équation $x^3 + y^3 = z^3$; on voit alors facilement que 3 divise x, y ou z .

En présentant les choses négativement (raisonnement par l'absurde), on prouverait le premier cas de Fermat en disant que si p ne divise pas xyz , alors l'équation $x^p + y^p = z^p$ est impossible. Comme zéro est divisible par tous les nombres, y compris p , les solutions tri-

viales sont éliminées d'emblée. Cet avantage se retrouvera dans la méthode de Andrew Wiles.

Dans le second cas, beaucoup plus difficile, il s'agit de démontrer que, non seulement p divise xyz , mais que toutes les puissances de p divisent xyz , ce qui implique que xyz est égal à 0 (un nombre non nul n'étant pas indéfiniment divisible).

Fermat avait trouvé une «route tout à fait singulière» pour résoudre le second cas et d'autres problèmes de cette nature : la «descente infinie» (voir *De Diophante à Fermat*, par Christian Houzel, *Pour la Science*, janvier 1996).

La descente infinie est un ingrédient essentiel de toutes les preuves classiques du «second cas» du théorème de Fermat, alors qu'elle est inutile pour le «premier cas», comme nous l'avons vu. Ici une véritable mutation va se produire : la méthode de A. Wiles traitera d'un seul coup de baguette magique les premier et deuxième cas, et ceci pour tous les exposants à la fois.

Finalement, en 1985, au moment où l'Histoire semblait hésiter entre tradition et idées à venir, trois hardis mousquetaires, Adleman, Fouvry et Heath-Brown essayèrent de régler définitivement le sort du premier cas. S'ils échouèrent, du moins échouèrent-ils avec panache : ils démontrèrent le premier cas pour une infinité d'exposants premiers. Ce résultat fit beaucoup de bruit, mais les mathématiciens savaient qu'il s'agissait d'un combat

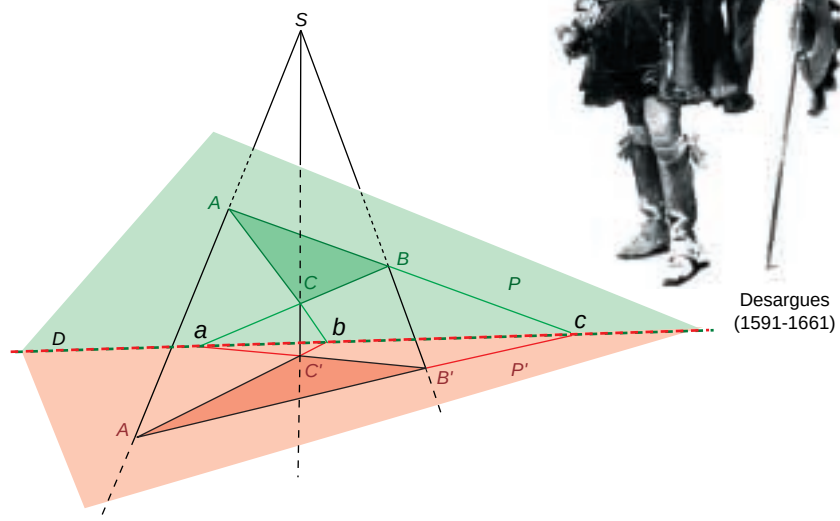
d'arrière-garde et que les batailles futures allaient se livrer sur d'autres fronts.

Le groupe de Galois absolu

À l'époque de Kummer déjà, les nombres algébriques avaient fait leur apparition dans l'étude du théorème de Fermat. Nous allons définir ces nombres mystérieux qui vont jouer un rôle essentiel.

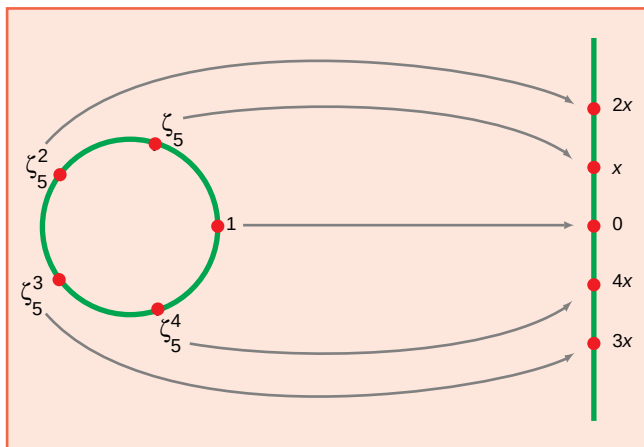
Un titre plus romantique pour ce sujet pourrait être «le corps des nombres algébriques et les représentations de son âme». En effet, la philosophie qui sous-tend ce type de question a d'abord été rêvée par Évariste Galois à la prison de Sainte-Pélagie (en 1831) avant de trouver sa consécration officielle dans le programme d'Erlangen de Félix Klein (en 1872). Cette philosophie consiste à attacher, à tout objet mathématique muni d'une structure, le groupe des transformations de cet objet qui respectent cette structure. On appelle ce groupe, le groupe des automorphismes de l'objet.

Si l'objet est l'ensemble des trois sommets d'un triangle isocèle (et non équilatéral) et sa structure la distance

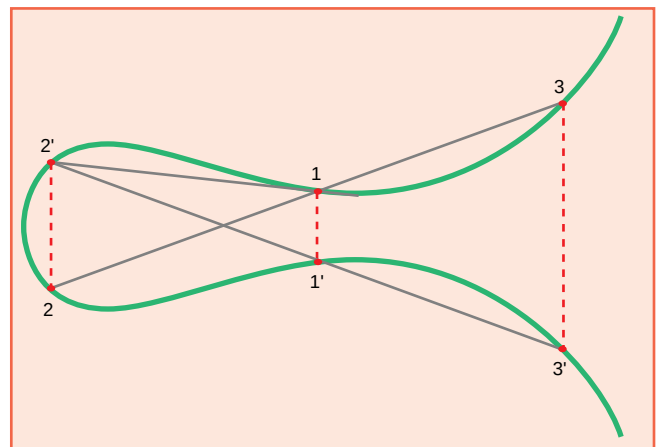


Desargues
(1591-1661)

1. LES GÉNÉRALISATIONS à des dimensions supérieures sont des moyens puissants de démonstration. Ainsi des propriétés de figures planes ne sont que les ombres de propriétés de figures dans l'espace. Si SAA', SBB', SCC' sont alignés, alors a, b, c le sont aussi. Ce théorème, dû à Desargues, est démontré facilement en donnant du relief à la figure : celle-ci est considérée comme la projection plane de deux triangles en perspective dans l'espace, les triangles ABC et $A'B'C'$, situés dans deux plans distincts, P et P' . Alors les points a, b, c sur la droite d'intersection D des plans P et P' , sont alignés.



2. LES CINQ POINTS SUR LE CERCLE représentent les points de 5-division du groupe T . Les flèches envoient ces cinq points sur une droite dont les points sont repérés par les entiers modulo 5. Au produit de ζ^2 par ζ^4 sur le cercle, donnant le point ζ , correspond l'addition de $2x$ à $4x$, soit $6x$ modulo 5, ou encore x . Pour démontrer le théorème de Fermat d'exposant p (ici 5), on utilise les points de p -division d'une courbe elliptique liée à une solution hypothétique de l'équation de Fermat.



3. À PARTIR DE DEUX POINTS 1 ET 2 de coordonnées rationnelles sur une courbe elliptique, on détermine un point 3, intersection de la droite passant par 1 et 2 avec la courbe, dont les coordonnées sont également rationnelles. Le point $3'$, symétrique du point 3, est le composé des points 1 et 2, et cette règle de composition définit une structure de groupe. La composition d'un point, 3 par exemple, avec le point à l'infini revient à prendre le point symétrique de $3'$ par rapport à l'axe de symétrie de la courbe : on retrouve le point 3 lui-même.

entre ses sommets, les transformations qui conservent l'objet et sa structure, les automorphismes, sont l'identité et la symétrie évidente.

Ainsi, lorsque l'objet est un anneau, la structure est formée par l'addition et la multiplication ; les automorphismes de l'anneau sont les transformations qui font correspondre à un élément de l'anneau un autre élément de l'anneau, en respectant ces deux lois.

Les nombres algébriques sont les nombres complexes qui sont solutions d'une équation polynomiale à coefficients fractionnaires : l'équation $3x^2 - 4$ a pour solutions $2\sqrt{3}/3$ et $-2\sqrt{3}/3$; ces nombres sont algébriques. Il est patent que les nombres rationnels sont algébriques. Le nombre π n'est solution d'aucune équation polynomiale à coefficients fractionnaires non nuls, il n'est donc pas algébrique ; on dit qu'il est transcendant.

Les mathématiciens ont démontré que les nombres algébriques constituent un corps (la somme et le produit de deux nombres algébriques sont des nombres algébriques).

Prenons par exemple un nombre complexe z que l'on obtient par des additions, soustractions, multiplications et divisions des nombres rationnels et du nombre complexe $\zeta_5 = e^{2i\pi/5}$. Le nombre z est algébrique parce que le nombre ζ_5 lui-même est algébrique. En effet, ζ_5 vérifie l'équation polynomiale à coefficients rationnels : $x^4 + x^3 + x^2 + x + 1 = 0$. Cette équation ne peut être décomposée en produits de polynômes à coefficients rationnels.

L'ensemble des nombres obtenus de la même manière que z forme le corps cyclotomique d'ordre 5 (ou corps de la division du cercle en cinq parties égales). C'est un sous-corps du corps de tous les nombres algébriques.

Dans notre théorie, ce corps possède un groupe d'automorphismes, le groupe des transformations de ce corps en lui-même, qui respectent l'addition et la multiplication. Ce groupe est appelé le groupe de Galois de notre corps cyclotomique.

Les automorphismes du corps des rationnels se réduisent à l'identité : ils ne sont pas très intéressants. Par chance, ζ_5 appartient à la famille des quatre frères jumeaux $e^{2i\pi/5}$, $e^{4i\pi/5}$, $e^{6i\pi/5}$, $e^{8i\pi/5}$ qui vérifient l'équation précédente. Le groupe de Galois de notre corps cyclotomique a donc quatre éléments.

La méthode utilisée par Kummer pour étudier l'équation de Fermat de degré 5 est déjà un magnifique exemple de l'utilisation de certains nombres cyclotomiques.

Le groupe des automorphismes de l'énorme corps de tous les nombres algébriques est appelé le groupe de Galois absolu. Malheureusement on ne connaît guère de caractéristiques de ce groupe de Galois absolu. C'est un objet aussi fondamental que mystérieux, mais il n'en sert pas moins de leitmotiv à la grande symphonie orchestrée par A. Wiles. Je vous entends vous exclamer : si le groupe de Galois absolu reste une notion métaphysique, comment en dire des choses positives, falsifiables ? En

reprenant l'exemple ci-dessus, on voit que tout automorphisme appartenant au groupe de Galois absolu se reflète dans le groupe de Galois du corps cyclotomique bâti à partir du nombre ζ_5 .

En réalité, ce que l'on fait avec le nombre 5 peut être fait avec tout entier positif n . Les points ζ_n ont leur image sur le cercle unité du plan complexe et ce cercle est muni naturellement d'une loi de groupe commutatif par la multiplication d'un nombre complexe. Ce groupe des nombres complexes de module 1 est désigné par T .

Le point ζ_5 est un élément de T tel que $\zeta_5^5 = 1$: on dit que c'est un point de 5-division de T . L'ensemble des éléments ζ qui vérifient cette condition forme un sous-groupe cyclique d'ordre 5 de T . Ce que l'on a étudié plus haut était l'action du groupe de Galois absolu sur ce sous-groupe. Ce sous-groupe étant isomorphe à une droite (voir la figure 2) sur le corps à cinq éléments F_5 , on a ainsi effectué une représentation linéaire du groupe de Galois absolu sur une droite.

Les représentations du groupe de Galois absolu ont toujours fasciné J.-P. Serre ; dans les années 1970, il s'intéressait à un type analogue de représentations : celles du groupe de Galois absolu agissant sur le groupe des points de p -division d'une courbe elliptique dont les coefficients de l'équation sont rationnels. Nous examinerons plus loin ces courbes elliptiques.

Les points du cercle T sont paramétrés par une variable réelle modulo

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 cor-

respondre 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 :

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

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

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

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

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 :

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

qui lui permet 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 $-2, -4, -6, \dots$, 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 :

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

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 :

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

On vérifie que

$$T_l(f) = af,$$

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 :

$$f[\exp(\alpha\tau + b/c\tau + d)] = (c\tau + d)^2 f[\exp(\tau)],$$

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 points 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-

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.

Partage de butin

IAN STEWART

Des protocoles de partage proportionnels, plaisants ou partiels.

Arthur Barberousse renversa le sac sur la table de la cuisine. Jo le Teigneux, Denis Tourtencuisse et Léon la Volette regardaient, émerveillés, les paquets de billets et les tas de bijoux qui en sortirent. Restait le plus difficile : diviser le butin. Personne n'avait confiance et chacun voulait avoir sa part, sans être lésé. La justice, c'est la justice, n'est-ce pas ?

Arthur partagea rapidement l'argent, en se fondant sur la valeur affichée. C'était facile : il suffisait de diviser la valeur totale en quatre. En revanche, le partage des bijoux était plus épineux, car chaque membre de la bande avait son idée sur la valeur des divers bijoux. Certains objets, telles les chaînes, pouvaient se couper en morceaux, ce qui facilitait le travail, mais les autres...

«Ne traînons pas, dit Jo. La police doit être sur nos traces, et tout cela doit disparaître rapidement.

– Je vais prendre cette tiare de diamants, dit Léon, en se la mettant sur la tête. Et Jo aura les colliers et le...

– Pas question, intervint Denis : des canailles de votre espèce ne seront jamais d'accord si elles procèdent ainsi. Il faut une méthode qui nous garantisse à chacun un partage équitable.

– Ouais, dit Léon.

Silencieux, ils regardèrent le tas de bijoux. Trois heures après, ils le regardaient encore :

«Ce dont nous avons besoin, dit Denis, c'est de ce que les mathématiciens nomment un "protocole de partage proportionnel plaisant", PPPP en abrégé.

– Aïe, dit Arthur. Et c'est quoi, ce truc ?

– Plaisant, c'est lorsque personne n'a le sentiment que quelqu'un d'autre a obtenu quelque chose qu'il ne...

– Je comprends "plaisant", mais les longs mots d'avant ?

– Un "protocole de partage", c'est une méthode systématique pour partager les choses entre plusieurs personnes. Il est "proportionnel" si chaque personne est satisfaite d'avoir reçu au moins sa juste part, et si personne n'estime qu'un autre a eu plus que sa part.

– N'est-ce pas la même chose que plaisant, demanda Léon ?

– Pas du tout.

– Oui, ajouta Denis. Les protocoles plaisants sont toujours proportionnels, mais les protocoles proportionnels ne sont pas nécessairement plaisants.

– Pourquoi ?

– Par exemple, suppose que, tous les trois, vous partagiez trois objets, comme un bracelet, un collier et une paire de boucles d'oreilles, et que vous assigniez subjectivement des valeurs de la façon suivante :

	Bracelet	Collier	Boucles
Arthur	40	50	10
Léon	30	50	20
Jo	30	20	50

Le partage est proportionnel si Arthur reçoit le bracelet, si Léon a le collier et si Jo a les boucles, parce que chacun d'entre vous aura reçu plus de 33 pour cent de la valeur totale, mais Arthur ne trouvera pas plaisant que Léon ait le collier, qu'il estime valoir plus que le bracelet. Comme nous le verrons, les protocoles plaisants sont beaucoup plus difficiles à trouver que les protocoles proportionnels.

En plus du protocole, des stratégies personnelles garantissent à chacun qu'il atteigne son but. Ces stratégies ne font pas partie du protocole ; elles sont d'ailleurs souvent implicites, mais ce sont elles qui garantissent que le protocole est juste. On nomme souvent "joueurs" les personnes entre lesquelles s'effectue le partage, parce qu'on peut envisager ce dernier comme une suite de coups dans un jeu, et l'on peut aussi représenter les valeurs comme des parts d'un gâteau. On se partage le gâteau, quoi.

Pour deux joueurs, par exemple Arthur et Léon, il existe un PPPP simple, que j'appelle «je coupe, tu choisis» : Arthur coupe le gâteau en deux parts égales, et Léon choisit celle des deux parts qu'il préfère. Avec ce protocole, la stratégie d'Arthur doit être de couper des parts égales à son goût, de sorte qu'il ne puisse perdre, quel que soit le choix que fera Léon. Pour Léon, la stratégie doit être de choisir la part qui lui semble la plus grosse. La stratégie d'Arthur lui assure une part qu'il estime à 50 pour cent, et celle de Léon une part que Léon estime supérieur ou égale à 50 pour cent. Le protocole est bien un PPPP.

Comme Denis semblait bien connaître le problème, les trois autres l'envoyèrent à la bibliothèque de l'université locale pour y dénicher des informations supplémentaires et authentifiées. Denis découvrit que les mathématiques des partages naquirent dans la Pologne en guerre, à Lvov : en 1944, alors que l'armée soviétique combattait pour reprendre la Pologne aux Allemands, le mathématicien Hugo Steinhaus chercha à se changer les idées en résolvant un problème de partage. Il connaissait le protocole «Je coupe, tu choisis» pour partager le gâteau entre deux personnes et les stratégies conduisant chacune d'elles à penser que sa part est au moins égale à la moitié. Avec cette technique, aucun des deux joueurs n'a de raison de se plaindre : celui qui coupe peut faire une découpe impartiale, et celui qui choisit décide ce qu'il veut prendre ; aucun des deux n'est forcé de faire un choix qu'il jugerait injuste.

«Steinhaus, dit Denis quand il revint vers ses trois acolytes, se demanda si on pouvait diviser un gâteau entre trois personnes.

– Voyons, dit Arthur. Peut-être pourrais-je couper le gâteau en trois parts que j'estimerai égales, puis faire choisir Léon et ensuite Jo ?

– Non, protesta Jo : je ne marche pas, car je choisirais ainsi après Léon, et je risquerais d'avoir une part moins grosse que la sienne.»

Denis expliqua alors que Steinhaus avait abouti à une suite de neuf étapes à l'issue de laquelle chaque joueur est satisfait, car il a ce qu'il considère être au moins un tiers du gâteau. Afin d'examiner ce protocole proportionnel, procédons à quelques définitions. Un joueur estime qu'une part est «juste» si la taille de cette part lui semble au moins égale à un tiers ; sinon elle est «injuste». «Passer», à une certaine étape du protocole, c'est ne rien faire. Par commodité, nous parlerons de «taille des parts», mais il s'agit de valeur relative, estimée par un joueur. Tous les jugements sont subjectifs et propres au joueur qui a le trait. Les indications entre parenthèses ne font pas partie du protocole ; ce sont des commentaires sur les stratégies utilisées par les joueurs.

Voici maintenant le protocole de Steinhaus (voir la figure 1) :

1. Arthur coupe le gâteau en trois parts (qu'il juge toutes justes, c'est-à-dire subjectivement égales).

2. Léon peut : soit passer (s'il pense qu'au moins deux parts sont justes) ; soit étiqueter deux parts (qu'il juge injustes) comme «mauvaises».

3. Si Léon passe, Jo choisit une part (qu'il estime juste). Puis Léon choisit une part (qu'il estime juste) et, finalement, Arthur prend la dernière part.