LE DERNIER THÉORÈME DE FERMAT

PHILIPPE LANGEVIN

Résumé. Pour les « fêtes de la science » de cette année des mathématiques, je vous propose un petit voyage au coeur d'une des plus anciennes disciplines scientifiques, l'étude des nombres, sur les sentiers du dernier théorème de Fermat. Le texte est conçu pour satisfaire l'appétit de tous : collégiens, lycéens, étudiants et amateurs des mathématiques. Quelques passages sont assez délicats, disons même difficile, voire obscures, mais « mathêma » n'est pas toujours une partie de plaisir et il faut apprendre à sauter les obstacles pour voir plus loin que le bout de son nez. L'objectif principal est de nature historique et « humaniste », convaincre le lecteur que la science actuelle doit tout aux anciens même si ces premiers ne savaient pas tout. La dernière partie du document donne quelques éléments de la démonstration du théorème de Fermat. Une preuve complexe du XX^{e} siècle qui s'appuie sur les publications d'un très grand nombre d'arithméticiens et géomètres contemporains. Pour en savoir plus, les étudiants et amateurs de mathématiques sont invités à parcourir la toile à partir du site de Kenneth Ribet.

Table des matières

1. En travaux

Le logo ci-contre réalisé par mon collègue de travail Jean-Pierre Zanotti est présent ici et ailleurs pour vous avertir que ce document est encore en construction. La fin des travaux est espérée pour l'an 1 ou 2. Mais j'imagine que certains lecteurs pourront tirer partie de ces notes. Je les invitent à me faire part de leurs suggestions, corrections et critiques.

`langevin@univ-tln.fr`

Dernière modification : octobre 2004.

2. Prologue

Au milieu du XVII^e siècle, le toulousain Pierre de Fermat consigne dans les marges de son exemplaire des arithmétiques de Diophante une séries de résultats sur les nombres et leurs propriétés cachées, des défis à destination de ses successeurs. Un siècle après lui, Léonard Euler les relève un à un mais reste impuissant face l'un d'entre eux, tout comme des générations de mathématiciens professionnels et amateurs qui tenteront leur chance sur cette proposition qu'on a pris l'habitude d'appelée le « dernier théorème de Fermat ». La proposition de Fermat affirme que l'équation $x^n + y^n = z^n$ est impossible à satisfaire en nombres entiers (strictement) positifs pour tous les exposants autres que un et deux. Un énoncé très simple, compréhensible par tous, et susceptible d'éveiller la curiosité de n'importe quel mathématicien débutant. Dans ses notes personnelles Fermat déclare en avoir établi la preuve par une méthode remarquable : la descente infinie. Dans ses correspondances, on retrouve effectivement une démonstration subtile mais qui ne traite que de l'exposant 4. Ses successeurs tenteront de reconstruire la preuve générale, seuls les cas des petits exposants seront résolus au prix d'efforts intenses : Euler ($n = 3$), Dirichlet et Legendre ($n = 5$) et Lamé ($n = 7$). Il est intéressant de noter que Gauss, le plus grand arithméticien de tous les temps, ne publie rien sur cette question. Sans doute pris en tenaille par sa devise « peu mais mûr » et l'inextricable énigme de Fermat. Sur cette question comme d'autres de même nature, il distribue des conseils et des encouragements aux mathématiciens qui prennent contact avec lui. L'unique mathématicienne de cette période, Sophie Germain, reçoit tous ses honneurs et félicitations pour son approche suffisamment générale qui traite de ce qu'on appelle aujourd'hui le premier cas de l'hypothèse de Fermat.

Au cours du printemps 1847, Lamé déclare posséder la démonstration du grand théorème de Fermat, une preuve générale qui s'applique à tous les exposants. Son raisonnement s'appuie sur la factorialité des anneaux cyclotomiques, un résultat intermédiaire qu'il pense pouvoir établir sans trop de difficulté avec l'aide de Cauchy. Un mois plus tard, Kummer démonte les certitudes des deux hommes en donnant un contre-exemple qu'il avait publié trois ans auparavant : l'anneau $\mathbf{Z}[\zeta_{23}]$ n'est pas factoriel ! Il explique cependant savoir comment se passer de cette condition de factorialité par l'intervention d'une notion nouvelle, celle des nombres complexes idéaux. Le théorème de Fermat est établi pour tous les exposants premiers vérifiant une condition de régularité, le nombre 37 est le plus petit exposant qui passe les mailles de son filet. Les arithméticiens du début du XX^e siècle affineront la méthode de Kummer. En 1993 l'hypothèse de Fermat est vérifiée pour tous les exposants inférieurs à 4 millions, un nombre respctable mais négligeable devant l'infinité des nombres premiers. Dans sa conférence du 23 juin 1993, le mathématicien Andrew Wiles annonce la démonstration de d'une conjecture formulée par Taniyama au milieu des années 50. Tous les spécialistes présents sont conscients des conséquences de ce résultat quand il est juxtaposé avec l'astuce des courbes elliptiques suggérée par Hellegouarch (1970), la brillante idée de Frey (1984), les conjectures de Serre (1972-1987), la démonstration par Ribet de la « conjecture epsilon » en 1992, et la contribution de dizaines d'autres de nos contemporains. Une vive émotion envahit l'auditoire, les applaudissements sont relayés par des centaines de mails qui circulent sur internet, en quelques minutes la communauté scientifique prend connaissance de l'événement : le théorème de Fermat venait tout juste de tomber.

Quelques mois après, Katz chargé de vérifier point par point le raisonnement de Wiles demande des précisions sur un passage du manuscrit de Wiles. L'auteur comprend que son collègue vient de mettre le doigt sur une faille, une erreur de raisonnement dans l'emploi des méthodes de Flach et Kolygavin. Pour éviter l'effondrement de l'édifice Wiles unit ses efforts avec Taylor, deux ans après la preuve est réparée. Voilà, le théorème de Fermat né à Toulouse en 1641, est donc definitivement tombé entre Cambridge et Princeton en 1995.

3. Avant-Propos

Pour la première fois depuis leur création par le ministère de la recherche et de l'éducation nationale, l'université de Toulon participe aux journées sciences en fête. Une semaine pour les sciences dans le cadre de l'année des mathématiques. Une série d'évènements inédits qui met « mathêma » sous le feu des projecteurs, une situation unique qui mérite bien quelques efforts, et cette note écrite spécialement pour l'occasion représente ma contribution. Un document illustré par, ou pour illustrer, la projection du film de Sing et Lynch "Last Fermat Theorem", voir [14]. Prévenu tardivement de la participation de l'UTV à ces journées, cela ajouté à l'incompétence de l'auteur sur le sujet explique la faiblesse du document sur le fond et sur la forme. Le lecteur est invité à soumettre ses critiques et améliorations à `langevin@univ-tln.fr`.

La démonstration du théorème de Fermat est très difficile, seulement une petite poignée de mathématiciens peuvent comprendre tous les tenants et aboutissants de la preuve de Wiles. Il n'empêche que le sujet peut-être approché par tous. L'objectif de cette note est de faire voyager le lecteur au coeur d'une des plus anciennes disciplines scientifiques, la théorie des nombres sur les traces des plus grands arithméticiens en quête du Graal de la théorie des nombres. Le texte est conçu pour satisfaire à l'appétit de tous : collégiens, lycéens, étudiants et amateurs des mathématiques. Quelques passages sont assez délicats, mais mathêma n'est pas toujours une partie de plaisir et il faut apprendre à sauter les obstacles. Les voyages forment la jeunesse, celui-ci de nature à la fois humaniste et historique nous aide à comprendre l'importance des anciens : ils n'ont pas tout su mais nous leurs devons tout.

Philippe Langevin, le 15 octobre 2000.

4. Pourquoi faire ?

Nous l'avons dit dans l'introduction, si n désigne un entier supérieur à 2 alors l'équation de Fermat

$$X^n + Y^n = Z^n$$

est impossible, c'est-à-dire qu'il n'existe pas de triplet (a, b, c) en nombre entiers strictement positifs vérifiant $a^n + b^n = c^n$. Il s'agit du grand théorème de Fermat établit par le concours de plusieurs centaines de mathématiciens, au prix de plusieurs millions d'heures de réflexion consommées entre la date de son énoncé 1641 et celle de sa preuve 1995.

Le théorème de Fermat ne sert à rien, plus précisément ne sert encore à rien. Personne ne peut dire s'il servira un jour à quelque chose. Ma réponse déçoit sans doute l'honnête lecteur, et réjouit l'utilitariste qui voit déjà un moyen de faire suspendre quelques cours fondamentaux de plus. Allez, vive la pratique et abat la théorie ! Place aux incubateurs et aux promoteurs des nouvelles technologies de l'information et des communications ! Hola, du calme, ne nous emballons pas si vite. Laissons de cté les aspects mercantiles de la recherche scientifique. Le théorème de Fermat est avant tout une énigme, une énigme mathématiques mais une énigme. Une question matière à réflexion qui sert effectivement à réfléchir, tout bêtement. La perméabilité du monde des idées qu'elles soient scientifiques, littéraires, artistiques, fait que quelque part les recherches sur ce genre de question influences et font progresser d'autres domaines et inversement. La preuve de Wiles est une oeuvre du XX^e siècle, conséquence de l'ensemble des activités humaine. Mon discours elliptique n'aura pas convaincu mais l'étroitesse de cette section m'empêche de développer davantage le fil de mes idées. Rendez-vous au café de la science, en attendant, pour satisfaire la curiosité utilitariste légitime du lecteur, je vais m'aventurer dans un exemple concret, celui des nouvelles technologies !

Les techniques de synchronisation de signaux utilisées dans les télécommunications numériques utilisent des signaux particuliers faiblement auto-corrélés et inter-corrélés. La transformée de Fourier permet reformuler les questions d'existence et de constructions de ces signaux dans le langage des équations diophantiennes où toutes les techniques mise au point pour la résolution du grand théorème de Fermat s'appliquent. Nous venons de mettre en évidence un lien invisible entre l'équation de Fermat et le bout de l'antenne de votre téléphone cellulaire...

5. Souvenirs de collégien

Que nous reste il de nos premiers cours de mathématiques ? Une certaine intuition des nombres, la découverte des entiers négatifs et des nombres à virgules, nos premières équations à une inconnue, les identités remarquables. Les droites, les triangles, les parallélogrammes et autres figures associées le plus souvent à quelques patronymes exotiques : Thalés, Euclide et Pythagore. Le temps passe et une petite phrase résiste à l'érosion de notre mémoire,

fait 1. *Le carré de l'hypoténuse est égal à la somme des carrés des autres côtés.*

Le fameux théorème de Pythagore qui relie les longueurs des petits côtés x et y d'un triangle rectangle à l'hypoténuse z, la corde tendue sous les angles, en une seule équation :

$$x^2 + y^2 = z^2. \tag{1}$$

Un pont-aux-ânes riche de conséquences, du maçon qui utilise l'instance $3^2 + 4^2 = 5^2$ pour vérifier sans équerre la rectitude d'un angle, à l'une des plus formidables aventures arithmétiques comme nous allons le montrer tout à l'heure. Bref, une petite merveille qui mérite bien que nous en fassions une démonstration sur le champ. Alors, observez la figure (3). Une preuve purement géométrique probablement découverte par quelques savants babyloniens, c'est-à-dire, un bon millier d'années avant Pythagore !

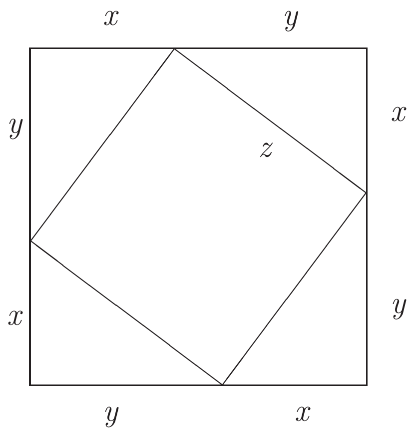

FIG. 1. Preuve géométrique de théorème de Pythagore.

6. Mathématiques antiques

Les mathématiques grecques naissent avec Thalés de Milet (-600) qui importe D'Égypte et Babylone des écrits sur les nombres et la géométrie. Mais c'est Pythagore de Samos (-500) qui fonde la démarche mathématique basée sur l'axiomatique et les raisonnements hypothéticodéductifs. Une philosophie axée sur la recherche des propriétés intrinsèques des nombres ces objets « abstraits » qui mesurent les longueurs, surfaces et volumes des figures géométriques et qui, d'après Pythagore, sont la source et le principe de toute chose.

Probleme 1. *Que dire de la nature du nombre mesurant la diagonale d'un carré dont le côté vaut une unité ?*

Par idéologie, l'école pythagoricienne privilégie la transmission orale du savoir et ne laisse aucun écrit. Une approche risquée qui, bien heureusement, est transgressée deux siècles plus tard par Euclide d'Alexandrie (-300), une sorte de Dieudonné des temps passés qui inscrit les mathématiques grecques dans une encyclopédie en treize volumes, les fameux *éléments*.

Le plus souvent inconnu des collégiens, bien après Euclide et peu avant le déclin de la civilisation grecque, un certain Diophante d'Alexandrie (+200) rédige ses *arithmétiques*, un recueil de problèmes en sept livres consacrés exclusivement aux nombres. Dans le sixième livre de ses arithmétiques, Diophante soumet à la sagacité de ses lecteurs :

Probleme 2. *Déterminer les triangles rectangles à côtés commensurables.*

En d'autre termes, il s'agit de résoudre l'équation (1) en nombre entiers i.e. Quels sont tous les triplets (x, y, z) d'entiers naturels satisfaisant à l'équation $x^2 + y^2 = z^2$? Une question relativement facile, à laquelle nous allons répondre par des méthodes élémentaires : identités remarquables du second degré, plus quelques considérations sur la divisibilité.

7. Les nombres

Le lecteur arrivé jusqu'ici sait tout de l'algèbre et des propriétés arithmétiques que je vais rappeler dans cette section. Qu'il ne se fâche pas et voit dans ces lignes qu'une sorte de mise en condition. Conformément à l'usage, nous désignons par $\mathbf{N}$ l'ensemble des entiers naturels et $\mathbf{Z}$ l'ensemble des nombres relatifs. Une notation empruntée à Dedekind (1831–1916) qui témoigne de la présence de école arithmétique allemande : Gauss, Jacobi, Dedekind, Dirichlet, Hilbert, Kronecker, Kummer, Weber etc. Pour plus de détails, je vous suggère la lecture de [1].

$$\mathbf{N} = \{0, 1, 2 \ldots\} \quad \mathbf{Z} = \{\ldots, -1, 0, 1, \ldots\}$$

Ces ensembles de nombres sont munis quatre opérations. On dit que l'entier d divise un entier z s'il existe un troisième q (le quotient) tel que $z = qd$ et, si abstraction faite du signe, d est différent de 1 et de z alors on parle de diviseur propre. Les entiers -1 et $+1$ divisent tous les autres, et ce sont les seuls à vérifier cette propriété, et on parle unités de $\mathbf{Z}$. Un nombre qui n'est pas une unité et qui ne possède pas de diviseur propre est dit *premier*. En effet, depuis Euclide, les mathématiciens ont de bonne raison de ne pas considérer première l'unité ! Deux nombres x et y sont dit *étrangers* ou *premiers entre-eux* s'ils ne possèdent pas de diviseur commun propre.

Exercice 1. *Si d divise deux entiers alors il divise leur somme et leur différences.*

Proposition 1 (Euclide)**.** *Si d est premier avec x et d divise le produit xy alors d divise y.*

Exercice 2. *Les premiers sont en nombre infini.*

Théorème 1 (Décomposition en facteurs premiers)**.** *Au signe et à l'ordre des facteurs prés tout entier se décompose d'une et une seule manière comme un produit de premiers.*

Corollaire 1. *Soient x et y deux entiers étrangers dont le produit est une puissance. Chacun d'eux pris séparément est une puissance du même ordre.*

Les philosophes grecs ignorent les entiers négatifs, des chimères qui deviendront réalités au milieu du XVI^e siècle. Mais, ils manipulent les fractions et donc les nombres rationnels (positifs), nous noterons $\mathbf{Q}$ le corps des nombres rationnels. Le moment est venu de donner une réponse au problème (1).

Démonstration. Notons x la mesure de la diagonale du carré unité. Le théorème de Pythagore affirme que $x^2 = 1^2 + 1^2 = 2$, x désigne une quantité bien réelle qui n'appartient pas au domaine des nombres rationnels. En effet, supposons le contraire, de sorte que x peut s'écrire sous la forme d'une fraction $x = \frac{a}{b}$, où a et b sont deux entiers étrangers vérifiant

$$a^2 = 2b$$

Le premier 2 divise a^2, il figure dans la décomposition de a^2, il divise a. Écrivons a sous la forme d'un double $a = 2\alpha$, l'égalité précédente devient

$$2\alpha^2 = b$$

et comme précédemment 2 divise b, ce qui est contraire à l'hypothèse et prouve le caractère irrationnel du nombre x qu'on note $\sqrt{2}$ depuis l'introduction du symbole $\sqrt{}$ par Christophe Rudolff en 1525 [6]. □

8. Triangles Pythagoriques

Soient x, y et z trois entiers satisfaisant à l'équation de Pythagore. Tout diviseur de deux de ces nombres divise le troisième. Quitte à diviser ces nombres par leur PGCD, on peut supposer x, y et z premier entre-eux deux à deux. Une analyse des parité montre que nécessairement l'un des trois nombres est pair.

Plus précisément, une analyse en congruence modulo 4 (voir plus loin, Lemme (1)) montre que ce n'est pas z et pour la suite, nous supposerons que c'est y. Par une petite manipulation algébrique faisant apparaître une identité remarquable, l'équation (1) devient

$$y^2 = (z - x)(z + x). \tag{2}$$

Les rationnels $\frac{z+x}{2}$ et $\frac{z-x}{2}$ sont des nombres entiers. Ils sont premiers entre eux. En effet, tout diviseur commun divise leur somme z et leur différence x, or par hypothèse x et y sont étrangers. Le corollaire (1) s'applique,

$$y = 2mn, \quad x = m^2 - n^2, \quad z = m^2 + n^2, \tag{3}$$

où m et n sont premiers entre-eux de parité distincte. Inversement, tout triplet $(\lambda x, \lambda y, \lambda z)$, avec λ arbitraire et (x, y, z) satisfaisant aux conditions ci-dessus est une solution du problème de Pythagore.

m	n	x	y	z
2	1	3	4	5
3	2	5	12	13
4	3	7	24	25

Proposition 2 (Fermat)**.** *Il n'existe pas de triangle rectangles dont les côtés soient rationnels et dont la surface soit un carré rationnel. En d'autres termes, l'équation :*

$$x^2 + y^2 = z^2, \quad \textit{et} \quad xy = 2t^2$$

ne possède pas de solution (x, y, z, t) *dans* $\mathbf{Q}^4$*.*

Cette affirmation que nous démontrerons un petit peu plus loin est équivalente à montrer l'impossibilité de résoudre en nombre entiers naturels le système :

$$\begin{cases} x^2 + y^2 = z^2; \\ xy = 2t^2. \end{cases} \tag{4}$$

9. Renaissance de l'arithmétique

Quelques siècles après Diophante, la civilisation grecque s'effondre, sa science et ses mathématiques avec. La fin dramatique d'Hépatie, la fille de Théon d'Alexandrie, mise en pièce dans les rues d'Alexandrie par un fanatique en témoigne, triste destinée d'une des rares contributrices aux sciences exactes de l'antiquité.

Au crépuscule de cette période obscure les oeuvres grecques se réfugient au pays des milles et une nuits, pour presque un millier d'années. Les mathématiciens arabes dont al-Kwaresmi (vers 800), abu Kamil (vers 850), al-Karaji (1000) et al-Khayyam (1048–1131) vont ajouter une représentation efficace des nombres et un ensemble des règles de manipulations des lettres et des chiffres : l'algèbre. Des mathématiques que Léonard de Pise (1170–1250) ramène de ses voyages en Afrique du nord. À partir de là, la résolution des équations algébriques devient une spécialité italienne avec les travaux de : Scipionne del Ferro (1465–1526), Tartaglia (1499–1557), Cardan (1501–1576) et Ferrari (1522–1565). La pratique des nombres et de l'algèbre envahit rapidement le continent Européen. Au XVI^e, quelques amateurs de mathématiques se lancent dans la traduction des ouvrages anciens, comme l'humaniste Xylander qui traduit intégralement les arithmétiques de Diophante. L'italien Rafael Bombelli (1526–1572), ingénieur en hydraulique illustre son traité d'algèbre par plus d'une centaine de problème de Diophante. Il décrit l'usage des nombres négatifs et des nombres imaginaires de ses prédécesseurs. En pleine guerre de religion, François Viète (1540–1603) et Gaspard Bachet (1581–1638) vont faire rentrer la France dans l'histoire arithmétique. François Viète mathématicien habile est recruté par les services du chiffres de Henri IV. Comme Bombelli, Viète extrait des résultats de Diophante pour illustrer l'efficacité de ses techniques d'algèbre. Claude Bachet de Méziriac effectue une traduction intégrale des textes de Diophante, techniquement plus affûté que Xylander, on lui doit notamment une première démonstration du théorème bien connu des apprentis algébristes :

Proposition 3 (Bachet-Bézout)**.** *Deux entiers a et b sont étrangers si et seulement s'il existe deux entiers relatifs u et v tels que $au + bv = 1$. De plus, on peut supposer $|u| < b$ et $|v| < a$.*

Une proposition fondamentale qu'il expose dans ses « problèmes plaisants et délectables ». Elle est redécouverte par Euler, puis étendue aux polynômes par Etienne Bézout (1730–1783). Une formule capitale qui en liaison lemme d'Euclide (1) contient les germes des « congruences » et de la théorie des corps finis. Il traduit en latin les travaux de Diophante qu'il commente de manière plus ou moins inspirée. La tâche n'est pas facile à cause du langage, des erreurs dues aux translations successives mais aussi à cause des erreurs numériques de Diophante lui même. Il remarque et formule la succulente énigme :

Théorème 2. *Tout nombre entier est une somme de quatre carrés.*

10. Vers la théorie des nombres

> *Il y a infinies questions de cette espèce, mais il y en a quelques autres qui demandent des nouveaux principes pour y appliquer la* descente, *et la recherche en est quelques fois si malaisée qu'on peut n'y peut y venir qu'avec une peine extrême. Telle est la question suivante que Bachet sur Diophante avoue n'avoir jamais pu démontrer, sur le sujet de laquelle M. Descartes fait dans une de ses lettres la même déclaration, jusque-là qu'il confesse qu'il la juge si difficile qu'il ne voit point de voie pour la résoudre. Tout nombre est carré ou composé de deux carrés, de trois ou quatre carrés. Je l'ai enfin rangée sous ma méthode et je démontre que si un nombre est point de cette nature, il y en aurait un moindre qui le serait pas non plus, puis un troisième moindre que le second, etc., à l'infini d'où l'on infère que tous les nombres sont de cette nature.*

Ce qui précède est un court extrait d'une lettre de Pierre de Fermat (1601–1665) adressée à Pierre de Carcavi (1600–1684), en août 1659. Une sorte de testament arithmétique dans laquelle Fermat explique sa méthode de démonstration favorite, la descente infinie, appliquée dans ce cours passage à la démonstration d'une proposition difficile. Dans cette lettre Fermat énumère des conséquences négatives et positive de sa méthode :

(1) Il n'existe pas de nombre, moindre de l'unité qu'un multiple de trois, qui soit composé d'un carré et d'un multiple de trois d'un autre carré.

(2) Il n'existe aucun triangle rectangle en nombres dont l'aire est un nombre carré.

(3) Tout nombre premier, qui surpasse de l'unité un multiple de 4 est composé de deux carrés.

(4) Tout nombre est carré ou composé de deux carrés, de trois ou quatre carrés.

(5) Aucun cube est divisible en deux cubes

(6) Il n'y a qu'un seul carré en entier qui, augmenté du binaire, fasse un cube. Le dit carré est 25. [$x^2 + 2 = y^3$.]

(7) Il n'y a que deux carrés en entiers, lesquels augmentés de quatre, fassent un cube. Les dits carrés sont 4 et 121. [$x^2 + 4 = y^3$.]

(8) Toutes les puissances carrées de 2, augmentées de l'unité, sont nombres premiers. [$F_n = 2^{2^n} + 1$.]

(9) Il n'y a que les deux nombres 1 et 7 qui, étant moindre qu'un double carré, fassent un carré de même nature, c'est-à-dire qui soit moindre de l'unité qu'un double carré.

Bachet se glorifie, en ses Commentaires sur Diophante, d'avoir trouvé une règle de résolution de l'équation $x^2 - Ay^2 = 1$ *dans deux cas particuliers ; je la donne générale en toute sorte de cas et détermine par règle si elle est possible ou non. J'ai ensuite rétablit la plupart des propositions défectueuses de Diophante et j'ai fait ce que Bachet avoue ne savoir pas et la plupart de celles auxquelles il paraît que Diophante à hésité, dont je donnerai des preuves et des exemples à mon premier loisir.*

*
* *

Voilà sommairement le compte de mes rêveries sur le sujets des nombres. Je ne l'ai écrit que parce que j'appréhende que le loisir d'étendre et de mettre au long toutes ces démonstrations et ces méthodes me manquera ; en tout cas, cette indication servira aux savants pour trouver d'eux-mêmes ce que je n'étend point, principalement si MM. de Carcavi et Frenicle leur font part de quelques démonstrations par la descente *que je leur ai envoyées sur le sujet de quelques propositions négatives. Et peut-être la postérité me saura gré de lui avoir fait connaître que les Anciens n'ont pas tout su, et cette relation pourra passer dans l'esprit de ceux qui viendront après moi pour* traditio lampadis ad filios, *comme parle le grand Chancelier d'Angleterre, suivant le sentiment et la devise duquel j'ajouterai :*

Multi pertransibunt et augebitur scientia

Les élèves et étudiants sensibles au charme de ces textes historiques sont invités à lire des détails dans les petits « Que-sais je ? » de Jean Itard [3] et [4], deux petits livres précieux.

11. Une marge historique

Avec le toulousain Pierre de Fermat, le champ de la connaissance des nombres s'élargit, des travaux qui marque une étape vers la théorie algébrique des nombres. Tous les problèmes qu'il liste dans sa lettre à Carcavi sont devenus des classiques et figurent dans tous les manuels de théorie des nombres cependant les preuves ont considérablement changé à l'image de celle qui concerne le théorème des quatre carrés, voir la preuve fondée sur les entiers d'Hurwitz(1859–1919) des corps de quaternions de Hamilton (1805–1865) proposée dans le cours de Samuel [5].

Il est impossible de partager soit un cube en deux cubes, soit un bicarré en deux bicarrés, soit en général une puissance quelconque supérieure au carré en deux puissances du même degré ; j'en ai découvert une démonstration véritablement merveilleuse que cette marge est trop étroite pour la contenir.

On retient de cette lettre l'enthousiasme de Fermat vis à vis d'un principe de démonstration, la descente infinie, un raisonnement inductif qu'il manipule pour contredire l'existence d'une solution à un problème diophantien. Il approfondit les commentaires de Bachet sur Diophante, un livre qu'il surcharge d'indications, de résultats consignés dans les marges, des défis lançés vers ses illustres successeurs qui ne manqueront pas de les relèver tous. La méthode à laquelle Fermat fait allusion, ses correspondances le prouvent, est fondée sur la descente infinie, il détaille le cas des bicarrés dans une de ses lettres mais personne n'a jamais trouvé de trace du cas cubique et encore moins du cas général.

12. La descente infinie

La descente infinie de Fermat s'apparente au raisonnement par récurrence. Pour montrer l'absence de solution à une équation $E(x, y, \dots)$, il suffit de prouver que l'existence d'une solution hypothétique (virtuelle) implique l'existence d'une autre de plus petite taille. Un mécanisme inférable à l'infini qui, au bout du compte, témoigne de l'absence de réelle solution.

Exemple 1. *Comme nous l'avons déjà démontré, l'équation $2x^2 = y^2$ est impossible en nombres entiers strictement positifs. Prouvons le par descente infinie.*

Démonstration. Partons d'une solution virtuelle (x, y). L'entier y est un double qu'on écrit $y = 2X$; Il apparaît que 4 divise $2x^2$ et donc que x est autre un double $x = 2Y$. Le couple d'entiers strictement positifs (X, Y) est moindre que (x, y) et vérifie la même équation. Un mécanisme qui se répète à l'infini alors qu'un ensemble d'entiers positifs bornés est fini. Une contradiction qui témoigne de l'impossibilité à résoudre $2x^2 = y^2$ en entiers positifs. □

Passons maintenant à la démonstration du fait (4).

Démonstration. Soit (x, y, z, t) une hypothétique solution. Les entiers x, y et z définissent un triangle pythagorique et, d'après ce que nous avons développé dans la section (8), il existe trois entiers λ, m et n tels que :

$$y = 2mn\lambda, \quad x = (m^2 - n^2)\lambda, \quad z = (m^2 + n^2)\lambda.$$

Par hypothèse, $\frac{xy}{2} = mn(m^2 - n^2)\lambda^2$ est un carré. Il en est de même les trois entiers m, n et $m^2 - n^2$ puisque ces derniers sont deux à deux premiers entre-eux.

Posons,

$$m = p^2, \quad n = q^2, \quad (p^2 - q^2)(p^2 + q^2) = r^2$$

Tout comme m et n, les entiers p et q sont étrangers de parité contraire et par conséquent $p^2 - q^2$ et $p^2 + q^2$ sont des carrés,

$$p^2 - q^2 = u^2, \quad p^2 + q^2 = v^2.$$

On a $(v-u)(v+u) = v^2 - u^2 = 2q^2$. Le PGCD de u et v vaut 2 et l'un des entiers $v-u$ ou $u+v$ est multiple de 4. On peut supposer que que ce soit $v-u$, de sorte que :

$$v - u = 4a^2, \quad v + u = 2b^2.$$

Et le triangle pythagorique $(b^2, 2a^2, p)$ est de surface carrée, et je laisse au lecteur le soin de vérifier qu'il est effectivement moindre que celui de départ ! $\square$

Corollaire 2. *(Fermat) L'équation diophantienne $x^4 + y^4 = z^4$ est impossible.*

Démonstration. En effet, nous pouvons supposer x, y et z deux à deux premiers entre eux. Il existe m et n deux entiers tels que $m^2 + n^2 = z^2$ et $2mn = y^2$: le triangle pythagorique (m, n, z) est de surface carrée, c'est absurde. $\square$

13. Congruence

Soit n un entier. On dit que deux entiers x et y sont congrus modulo n quand leur différence est un multiple de n. Il s'agit d'une relation reflexive, symétrique et transitive. En abrégé, on écrit $y \equiv x \mod n$, et donc

$$y \equiv x \mod n \Longleftrightarrow \exists k \in \mathbf{Z}, y - x = kn$$

Les relations de congruences sont capitales parcequ'elles satisfont des conditions de régularités. En effet, si $y \equiv x \mod n$ et $y^prime \equiv x' \mod n$ alors on a les congruences :

$$y + y' \equiv x + x' \quad \text{et} \quad yy' \equiv xx'.$$

Il s'agit d'un outil efficace pour mettre en évidence l'absence de solution à une equation diophantienne. Par exemple, le trinôme

$$1905X^2 + 1187X + 1$$

ne possède pas de racine entière. En effet, une hypothétique racine entière z, satisferait à $1905z^2 + 1187z + 1 = 0$ et donc, a fortiori, $1905z^2 + 1187z + 1 \equiv 0 \mod 2$. Or, modulo 2 l'expression $1905z^2 + 1187z + 1$ est équivalente à 1. Il faut comparer cette approche à la méthode brutale qui consiste à calculer le discriminant

$$1187^2 - 4 \times 1905 = 1401349$$

et vérifier que ce dernier est un nombre premier, d'où l'impossibilité.

Lemme 1. *Soient x, y et z trois entiers premiers entre eux formant un triangle Pythagorique*

$$x^2 + y^2 = z^2.$$

Un seul des entiers est pair mais z est impair.

Démonstration. On réduit la relation $x^2 + y^2 = z^2$ modulo 2 pour prouver qu'un des trois nombres est pair.Il suffit de constater que le carré d'un pair est congru à 0 modulo 4 et que le carré d'un impair est toujours congru à 1 modulo 4 pour arriver à la conclusion. □

14. Structure finie

Proposition 4 (Euclide)**.** *Soient a et b deux entiers positifs, si b n'est pas nul alors il existe un unique couple d'entiers (q, r) tels que :*

$$a = bq + r, \quad 0 \leq r < b.$$

Faire la division euclidienne de a par b c'est trouver le quotient q et le reste r satisfaisant aux conditions de la proposition ci-dessus.

Soit n un entier, et notons $[x]_n$ le reste de la division de x par n. Un résidu modulo n est un des restes possibles d'une division par n. Il exite n restes possibles, et donc n classes de congruences modulo n.

La proposition d'Euclide permet de munir l'ensemble des résidus modulo n de deux lois internes : une addition $\oplus$ et un produit $\otimes$.

$$x \oplus y = [x + y]_n, \quad x \otimes y = [xy]_n.$$

L'ensemble des résidus $\{0, 1, \ldots, n-1\}$ muni des opérations ci-dessus forme un anneau $\mathbf{Z}/n\mathbf{Z}$, c'est l'anneau des entiers modulo n. Rappelons qu'un corps est un anneau dans lequel un élément non nul est inversible. On démontre sans aucune difficulté que l'anneau $\mathbf{Z}/n\mathbf{Z}$ est corps si et seulement si n est premier. D'ailleurs, lorsque p est premier la tradition veut qu'on note $\mathbf{F}_p$ le corps $\mathbf{Z}/p\mathbf{Z}$.

Exercice 3. *Le groupe multiplicatif de $\mathbf{F}_p$ est cyclique d'ordre $p - 1$.*

Démonstration. Pas immédiat. □

Exercice 4 (Wilson)**.** *Montrer que $(p - 1)! = -1$.*

Démonstration. Facile. □

Tout comme le corps des nombres rationnels, le corps $\mathbf{F}_p$ possède une clôture algébrique Ω_p, une extension infinie de $\mathbf{F}_p$ composée des racines des polynômes à coefficients dans $\mathbf{F}_p$.

Proposition 5 (Division à reste minimal)**.** *Soient a et b deux entiers positifs, si b n'est pas nul alors il existe un unique couple d'entiers (q, r) tels que :*

$$a = bq + r, \quad |r| < b/2.$$

Exercice 5 (Gauss)**.** *L'anneau des entiers de Gauss $\mathbf{Z}[i] = \{a + ib \mid a, b \in \mathbf{Z}\}$ est euclidien par la norme $N(a + ib) = a^2 + b^2$. Plus précisément, si x et $y \neq 0$ désignent deux de ces entiers alors il existe un unique couple d'entiers de Gauss (q, r) tel que :*

$$x = qy + r, \quad N(r) < N(y).$$

15. Petit et grand théorèmes de Fermat

La démonstration qui précède n'est pas facile, et le lecteur fera bien de prouver le résultat qui suit par une descente infinie spécifique. D'où l'on tire que l'équation diophantienne $x^4 + y^4 = z^4$ est impossible.

Proposition 6. *(Fermat) L'équation diophantienne $x^4 + y^4 = z^2$ est impossible.*

Démonstration. Exercice ! □

Dans une marge de Diophante, Fermat signale une généralisation à tous les exposants. Mais cette généralisation n'est signalée nulle par ailleurs, alors que les cas des exposants 3 et 4 apparaissent à plusieurs reprises dans ses correspondances. On doit comprendre que Fermat ne fait que suggérer une hypothèse, une conjecture qui deviendra le « grand » théorème de Fermat.

Conjecture 1 (Grand théorème de Fermat)**.** *Pour tout entier $n > 2$, l'équation diophantienne $x^n + y^n = z^n$ est impossible.*

Une conjecture qu'on sait vraie depuis 1994 grâce à la « touche » finale de Andrew Wiles, soit trois siècles et demi après avoir été formulée. Une autre proposition plus élémentaire et prouvée effectivement par Fermat est associée au mathématicien Toulousain, le « petit » théorème de Fermat. Incomparablement plus élémentaire que le précédent, il n'en n'est pas pour autant moins utile ! Il est présent dans la majorité des questions d'arithmétique.

Théorème 3 (Petit théorème de Fermat)**.** *Soit p un nombre premier. Si p ne divise pas un entier a alors p divise $a^{p-1} - 1$.*

Démonstration. Exercice ! Le collégien pourra en faire une preuve dans le cas $p = 3$. Le lycéen fera une démonstration par récurrence. L'étudiant de licence argumentera de façon combinatoire alors que celui de maîtrise privilégiera la théorie des groupes et des anneaux. □

Dans le langage des congruences, le petit théorème de Fermat affirme que :

$$\forall a \in \mathbf{Z}, \quad a^p \equiv a \pmod p$$

dés que p est premier. Donnons une petite application du petit théorème de Fermat au cas de l'exposant 3.

Exemple 2. *Si $x^3 + y^3 = z^3$ alors 3 divise l'un des trois entiers x, y ou z.*

Démonstration. On peut partir de l'égalité $x^3 + y^3 = z^3$. Le petit théorème de Fermat montre que 3 divise $x+y-z$, il existe un entier k tel que $z = (x+y+3k)$ et donc

$$z^3 = (x + y + 3k)^3 \equiv x^3 + y^3 + 3xy(x + y) \pmod 9$$

et finalement 3 divise $xy(x + y)$. □

16. Quête d'une preuve

Contrairement aux scientifiques d'aujourd'hui, Fermat voyage peu et publie peu. Ses recherches demeurent mal connues malgrè les efforts de son fils Samuel Fermat qui rassemble et publie ses correspondances : observations de Pierre de Fermat sur les commentaires de Diophante de Gaspard Bachet de Méziriac. Un texte prit en considération par Léonard Euler (1707–1783) qui corrige les erreurs de

Fermat et améliore quelques démonstrations. Lui aussi est séduit par le probème des quatre carrés, pour résoudre le problème des quatre carrés, il invente une identité très spectaculaire :

$$(a^2 + b^2 + c^2 + d^2)(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) = A^2 + B^2 + C^2 + D^2$$

avec

$$\begin{aligned} A &= a\alpha + b\beta + c\gamma + d\delta & B &= a\beta - b\alpha + c\delta - d\gamma \\ C &= a\gamma - d\delta - c\alpha + d\beta & D &= a\delta + b\gamma - c\beta - d\alpha \end{aligned}$$

Exercice 6. *Facile à vérifier mais difficile à trouver !*

Euler utilise cette formule pour construire une une nouvelle preuve du théorème des quatre carrés, une démonstration qui devra à nouveau être améliorée par Lagrange. . .Euler montre que le point numéro (8) rapporté dans le court extrait de la section (10) est faux. En effet, le cinquième nombre de Fermat soit $2^{2^5}+1 = 4294967297$ n'est pas premier. Le voilà, sûr de l'existence de quelques failles dans les travaux de Fermat. Dans un premier temps, il pense que l'hypothèse est tout simplement fausse. Incapable de trouver une solution, il finit par se convaincre du contraire et se lance à la recherche de la preuve perdue. Sachant que de toute évidence, celle-ci est basée sur un argument de descente infinie. Il informe Christian Goldbach (1690–1764) de sa découverte le 4 aout 1753.

Théorème 4 (Euler, 1753)**.** *L'équation diophantienne* $x^3+y^3 = z^3$ *est impossible.*

Démonstration. Partons d'un triplet (x, y, z) composé de trois entiers premiers entre-eux et satisfaisant à l'équation $x^3+y^3 = z^3$. Comme dans le cas quadratique, un des deux entiers x ou y est pair, sans perdre en généralité, on peut supposer que c'est y.

$$y^3 = z^3 - x^3 = (z - x)(z^2 + zy + y^2)$$

Posons $u = \frac{z-x}{2}$ et $v = \frac{z+x}{2}$. Ce sont deux entiers premiers entre-eux et de parité opposée. L'équation devient

$$y^3 = 2u(u^2 + 3v^2)$$

Euler est un grand mathématicien. Pour aller plus loin dans cette factorisation, il propose d'agrandir l'espace de travail à l'ensemble des nombres de la forme $A+\sqrt{-3}B$. Un ensemble d'entiers algébriques, que nous notons **E**, et dans lequel on sait ajouter et multiplier depuis Bombelli :

$$\begin{aligned} (A + \sqrt{-3}B) + (A' + \sqrt{-3}B') =& (A + A') + \sqrt{-3}(B + B') \\ (A + \sqrt{-3}B) \times (A' + \sqrt{-3}B') =& (AA' - 3BB') + \sqrt{-3}(AB' + BA') \end{aligned}$$

L'arithmétique de **E** semble similaire à celle de **Z**. Pour l'essentiel, les unités de **E** sont 1 et -1. À l'image de 3 et 7, certains premiers de **Z** perdent leur caractère irréductible. Cependant, 2 et $\sqrt{-3}$ sont premiers dans **E**. Remarquons que si deux entiers sont étrangers, ils le demeurent dans le domaine algébriques.

Exercice 7. *Vérifiez ce que je viens de dire !*

Exercice 8. *Est-ce que l'égalité* $(1 + \sqrt{-3})(1 - \sqrt{-3}) = 4$ *vous interpelle ?*

Revenons au raisonnement d'Euler. Dans l'anneau algébrique, u^2+3v^2 se factorise en un produit de deux entiers algébriques conjugués

$$u^2+3v^2=(u+\sqrt{-3}v)(u-\sqrt{-3}v).$$

Soit d un diviseur commun de ces deux facteurs. Il divise leur somme $2u$ et leur différence $2\sqrt{-3}v$ mais ne peut être pair, c'est donc ± 1 ou $\pm\sqrt{-3}$.

Nous ne traitons que le cas $d=\pm 1$, l'autre cas est assez similaire.

$$y^3=(2u)(u+\sqrt{-3}v)(u-\sqrt{-3}v)$$

les trois termes sont deux à deux premiers entre-eux et sont nécessairement des cubes. En particulier, $2u$ est le cube d'un diviseur entier de y et

$$u+\sqrt{-3}v=(\alpha+\sqrt{-3}\beta)^3$$

et après développement du cube, on tire obtient :

$$\begin{aligned} u &= \alpha(\alpha-3\beta)(\alpha+3\beta) \\ v &= 3\beta(\alpha^2-\beta^2) \end{aligned}$$

Le raisonnement est douteux car 4 est une puissance égale à un produit de premiers distincts : $1+\sqrt{-3}$ et son conjugué. Cependant, je pourrais montrer qu'Euler a raison, en utilisant la théorie des anneaux de Dedekind. Mais la marge de ce document est trop étroite pour que je puisse donner plus d'explications.

Les entiers 2α, $\alpha-3\beta$ et $\alpha+3\beta$ sont deux à deux étrangers et comme leur produit $(2u)$ est un cube, nous en déduisons un triplet (X,Y,Z) tel que : $(XYZ)^3=2u$, $X^3=2\alpha$, $Y^3=\alpha-3\beta$, et $Z^3=\alpha+3\beta$. En particulier $X^3+Y^3+Z^3=0$ et fournit une solution moindre que (x,y,z). La descente infinie est amorcée. □

Exercice 9. *Traiter le cas $d=\pm\sqrt{-3}$.*

17. Exposant supérieur

Les recherches de Fermat et Euler, montrent que l'hypothèse de Fermat est vérifiée pour les exposants 3 et 4. Tout entier n supérieur à deux est multiple de quatre ou bien d'un premier impair, une considération qui permet de réduire le champ d'investigation aux exposants premiers impairs.

Conjecture 2 (Fermat, 1641)**.** *Soit p un nombre premier impair. Si x, y et z sont trois entiers relatifs tels que $x^p+y^p+z^p=0$ alors $xyz=0$.*

En toute généralité, nous pouvons supposer x, y et z deux à deux étrangers. La résolution du cas $p=3$ a été faite en deux temps, et en général, il apparaît nécessaire de séparer l'étude en deux cas.

Cas 1. p ne divise pas xyz.

Cas 2. p divise xyz.

 2.1 p divise x et 2 divise y.

 2.2 $2p$ divise x.

Les trois situations sont classées par ordre de difficulté. Après Euler, Johann Lejeune-Dirichlet (1805–1859) s'attaque au monstre et démontre le cas (2.1) de l'exposant 5, sa démonstration inspire Adrien-Marie Legendre (1752–1853) qui établit le cas (2.2) du même exposant, sans trop de difficulté malgrè son âge avancé. Les descentes infinies utilisées sont de plus complexe et ne peuvent pas figurées dans cette note. Le lecteur est renvoyé vers le livre d'Edwards [9]. Gabriel Lamé (1795–1870) ira un petit peu plus loin sur la piste de la descente infinie en démontrant les deux la conjecture dans le cas 7, une preuve probablement indigeste puisque presque jamais rapportée !

18. Sophie Germain

La mathématicienne Sophie Germain (1776-1831-) propose une alternative à la descente infinie, par une utilisation ingénieuse du petit théorème de Fermat. La proposition montre que si le premier cas de Fermat de l'exposant p est vérifié modulo un premier q, sujet à quelques conditions, alors le premier cas de l'hypothèse de Fermat est « globalement » vérifié.

Théorème 5 (Germain)**.** *Soit p et q deux nombres premiers impairs. Si p n'est pas une puissance p-ième modulo q et si*

$$\forall x, y, z \in \mathbf{Z} \quad x^p + y^p + z^p \equiv 0 \pmod q \Longrightarrow xyz \equiv 0 \pmod q$$

alors le premier cas de l'hypothèse de Fermat est vérifiée. En d'autres termes, $x^p + y^p + z^p = 0$ implique que p divise xyz.

Démonstration. Comme toujours, nous pouvons supposer x, y et z premiers entre-eux. En particulier, $(x+y)$ et $x^{p-1} - x^{p-2}y + \cdots - xy^{p-2} + y^{p-1}$ sont étrangers, et il existe deux diviseurs c et γ de z tels que :

$$x + y = c^p, \qquad c\gamma = z; y + z \qquad = a^p, a\alpha \qquad = x; z + x = b^p, \qquad b\beta = y.$$

L'égalité globale légalité modulo q et donc, un des trois entiers est divisible par q. Nous supposerons que c'est x. La somme des trois égalités ci-dessus donne

$$2x = c^p + b^p - a^p \equiv 0 \pmod q$$

l'un des entiers a, b ou c est donc divisible par q, une petite analyse montre que c'est forcément a. La seconde égalité montre que $z \equiv -y \pmod q$. Cette relation associée à $z^{p-1} - z^{p-2}y + \cdots - xy^{p-2} + y^{p-1}$ donne

$$pz^{p-1} \equiv \alpha^p,$$

une congruence impossible. □

Corollaire 3. *Si p et $2p+1$ sont premiers impairs alors le premier cas de l'exposant p est vérifié. On dit que p est un premier de Sophie Germain.*

Démonstration. Tout d'abord, p ne peut pas être une puissance p-ème modulo $q = 2p + 1$. Par l'absurde, si $x^p \equiv p \pmod q$ alors $x^{q-1} \equiv p^2 \pmod q$; d'un autre côté, le petit théorème de Fermat affirme que $x^{q-1} \equiv 1 \pmod q$. Deux congruences qui impliquent que q divise $(p^2-1) = (p-1)(p+1)$: c'est impossible. Vérifions le second point, si x , n'est pas divisible par q alors $x^{q-1} \equiv 1 \pmod q$ et nécessairement $x^p = \pm$ ce qui montre que $x^p + y^p + z^p$ ne peut-être nul modulo q si aucun des x, y, z ne l'est. □

19. Mais que fait Gauss ?

Le mathématicien Carl Friedrich Gauss (1777–1855) est incontestablement le chef de file des mathématiciens du XVIII^e qui lui transmettent régulièrement leurs résultats. Voici ce qu'il écrit à Sophie Germain lorsqu'il apprend qui se cache derrière un certain monsieur Leblanc.

> *Mais comment vous décrire mon admiration et mon étonnement de voir mon estimé correspondant Mr Leblanc se métamorphoser en cet illustre personnage* [Sophie Germain, à qui il écrivait après avoir découvert la supercherie] *qui donne un si brillant exemple de ce que j'aurais du mal à croire. Le goût des sciences abstraites en général et surtout des mystères des nombres est excessivement rare—ce n'est pas un sujet qui touche tout le monde—les charmes enchanteurs de cette sciences sublime ne se révèlent qu'à ceux qui ont le courage de s'y plonger profondément. Mais quand une personne du beau sexe, qui, selon nos coutumes et nos préjugés, doit rencontrer infiniment plus de difficultés que les hommmes à se familiariser avec ces recherches épineuses, réussit néanmoins à surmonter ces obstacles et à en pénétrer les parties les plus obscures, alors sans aucun doute, elle doit avoir le courage le plus noble, des talents tout à fait extraordinaires, et un génie supérieur. En vérité, rien ne pourrait me prouver d'une manière aussi flatteuse et moins équivoque que les attraits de cette sciences—laquelle a enrichi ma vie de tant de moments de bonheurs—ne sont pas chimériques, que la prédilection que vous avez témoignée à son égard.*

20. Les évènements de 1847.

Lors de la séance du 1er mars 1847 de l'académie des sciences de Paris, Gabriel Lamé annonce être en possession d'une voie nouvelle pour résoudre la conjecture de Fermat. Il résume la démonstration en expliquant que $x^n + y^n$ se factorise complètement dans l'ensemble des entiers augmenté de la racine n-ème principale, c'est-à-dire le nombre complexe $\zeta = \cos(2i\pi/n) + i\sin(2i\pi/n) = e^{2i\pi/n}$. Une idée qui aurait germée au cours d'une discussion avec Joseph Liouville (1809–1882) qu'il souhaite associer à cette découverte fantastique. Dans ce nouvel ensemble de nombres $\mathbf{A}_n$ qu'on appelle aujourd'hui l'anneau des entiers cyclotomiques d'ordre n, on obtient la factorisation :

$$x^n + y^n = (x+y)(x+\zeta y)(x+\zeta^2 y)\dots(x+\zeta^{n-1}y)$$

Lamé explique que l'anneau $\mathbf{A}_n$ est similaire à $\mathbf{Z}$ et qu'en particulier si tous les facteurs du membre de droite sont premiers entre-eux alors ce sont des puissances n-ème et qu'à partir de là, il est possible de procéder par descente infinie comme Fermat, Euler, Dirichlet, Legendre et lui même l'ont fait pour les petits exposants. Dans le cas contraire, il planifie de diviser les termes un diviseur commun pour arriver à ses fins. Après lui, Liouville prend la parole pour déclarer qu'il ne partage pas l'enthousiasme de Lamé. L'idée d'étendre le domaine des nombres pour obtenir une factorisation est excellente mais n'est pas nouvelle puisqu'elle remonte à Euler. De plus, la conjecture sur laquelle le raisonnement s'appuie, la décomposition en facteurs irréductibles dans $\mathbf{A}_n$, est plus que douteuse. L'exemple de l'anneau d'Euler en témoigne. Sur ce point crucial, Augustin Cauchy (1789–1857) partage complètement l'optimisme de Lamé. Il ne voit aucune obstruction majeure à la factorialité des anneaux cyclotomiques. Il ajoute avoir fait des recherches sur le sujet qui vont dans ce sens. La factorialité est acquise pour le degré 4, c'est un résultat de Gauss. Dans les semaines qui suivent, Wantzel (1814–1848) prouve celle du degré 3. Un résultat qui permet de réparer le raisonnement d'Euler puisque cet anneau contient les nombres d'Euler. Le 24 mai 1847, Liouville communique une lettre de Ernst Kummer (1813–1893) qui clôt le débat. Dans cette correspondance, Kummer explique que les anneaux cyclotomiques ne sont pas toujours factoriels le plus petit contre-exemple est $\mathbf{A}_{23}$, un fait qu'il détient probablement de Jacobi. Il précise que la factorialité n'est pas indispensable et que l'introduction d'une nouvelle notion, celle des « nombres complexes idéaux », permet d'arriver à une conclusion similaire. Bref, une très mauvaise journée pour Cauchy et Lamé.

21. Les nombres idéaux de Kummer

Pour faire plus court, j'expose dans cette section quelques résultats de Kummer, directement dans le langage des idéaux de Richard Dedekind (1831–1916). Le lecteur intéressé par le point de vue plus historique des « nombres idéaux de Kummer » peut consulter l'article de Terjanian paru dans la gazette de la SMF quelques mois après la chute du théorème de Fermat.

Rappelons qu'un anneau A est un ensemble muni de deux lois : addition et multiplication qui doivent vérifier des propriétés analogues à celles que nous connaissons dans le cadre des entiers relatifs. On dit qu'une partie I de A est un idéal si :

$$\forall x, y \in I, \quad x + y \in I, \qquad \forall a \in Ax \in I, \quad ax \in I$$

En d'autre termes c'est un sous-groupe additif de A stable par homothéties. L'ensemble des multiples de z forme un idéal, c'est l'idéal engendré par z. Un idéal P est dit premier lorsque l'appartenance $xy \in P$ ne peut se faire sans que $x \in P$ ou $y \in P$. Pour généraliser la notion de décomposition en facteurs premiers, on introduit le concept de produit d'idéaux. Soient I et J deux idéaux, les combinaisons linéaires des éléments de la forme ij avec $i \in I$ et $j \in J$ forment un idéal, c'est l'idéal produit IJ. Le produit des idéaux est associatif. Dans l'anneau $\mathbf{Z}$, tous les idéaux sont principaux et les notions de produit et de produit d'idéaux sont confondues. Les deux théorèmes qui suivent sont fondamentaux, ils se généralisent à tous les anneaux de Dedekind.

Théorème 6 (décomposition des idéaux)**.** *Soit A un anneau cyclotomique. Tout idéal I de A se décompose d'une et une seule manière en produit d'idéaux.*

Théorème 7 (Nombre de classes)**.** *Soit A un anneau cyclotomique. Il existe un entier h tel que pour tout idéal I, la puissance I^h est principale. Le plus petit $h > 0$ s'appelle le nombre de classes d'idéaux de A.*

Dans le cas de l'anneau cyclotomique $\mathbf{A}_p$, il est essentiel de démontrer quelques résultats intermédaires. Notons ζ une des racines p-ième primitive de l'unité. Les décompositions des idéaux principaux (p) sont $(\zeta - 1)$ liées, c'est une conséquence (inattendue ? !) du théorème de Wilson.

$$\big((\zeta-1)^p\big) = (p) = \mathfrak{P}_1^{p-1}\mathfrak{P}_2^{p-1}\dots\mathfrak{P}_g^{p-1}$$

et donc $(p) = \mathfrak{P}_1\mathfrak{P}_2\dots\mathfrak{P}_g$. Notons $\mathfrak{P}$ un quelconque de $\mathfrak{P}_i$. Deux racines p-ième distintes sont indépendantes modulo $\mathfrak{P}$. Si z est un entier cyclotomique arbitraire alors z s'écrit $z = \sum_{i=0}^{p-2} a_i\zeta^i$, et le petit théorème de Fermat montre que

$$z^p \equiv \sum_{i=0}^{p-2} a_i^p \equiv \sum_{i=0}^{p-2} a_i \mod \mathfrak{P}.$$

c'est-à-dire que z^p est équivalent à un entier rationnel modulo $\mathfrak{P}$. Enfin pour p supérieur à 5 alors pour toute partie $T \subset \{0, 1, \dots, p-1\}$ d'au plus 4 éléments alors $\sum_{i\in T} a_i\zeta^i \equiv 0 \mod \mathfrak{P}_i$ alors les entiers a_i sont tous nuls.

Exercice 10. *Il faut savoir démontrer ce qui précède pour la démonstration qui suit.*

Démonstration. Pour un dépannage, ouvrir le cours de Samuel. □

Proposition 7 (Kummer)**.** *Soit p un nombre premier. Si p ne divise pas le nombre de classe de l'anneau cyclotomique d'ordre p alors l'hypothèse de Fermat est vérifiée.*

Démonstration. Nous nous contenterons de prouver le premier cas de la conjecture de Fermat. Pour le deuxième cas, le lecteur peut consulter [9] ou encore [11]. Cela dit, il s'agit de démontrer qu'il n'existe pas de nombres entiers x, y, z étrangers deux à deux, premier avec p tels que $x^p + y^p = z^p$. Notons ζ la racine p-ème de l'unité, on obtient la factorisation :

$$x^p + y^p = \prod_{i=0}^{p-1}(x + \zeta^i y) = z^p.$$

Une égalité qui peut être vue comme une égalité d'idéaux principaux. Montrons qu'un idéal premier $\mathfrak{P}$ ne peut pas intervenir dans la décomposition de deux facteurs distincts. On peut supposer que 2 ne divise pas y de sorte que si $(x + \zeta^i y) \subset \mathfrak{P}$ et $(x+\zeta^j y) \subset \mathfrak{P}$ alors $2x \subset \mathfrak{P}$ et donc $x \in \mathfrak{P}$. Par ailleurs, $(\zeta^i - \zeta^j)y \subset \mathfrak{P}$, mais comme par hypothèse p ne divise pas x, il vient que $y \subset \mathfrak{P}$.

Nous en déduisons une factorisation idéale $(z) = \mathfrak{Q}_1\mathfrak{Q}_2\dots\mathfrak{Q}_p$ où les $\mathfrak{Q}_i$ sont étrangers deux à deux tels que $\mathfrak{Q}_i^p = (x+\zeta^i y)$. Comme le nombre de classes de $\mathbf{A}_p$ est premier avec p, la puissance $\mathfrak{Q}_i^p$ ne peut être principale sans que $\mathfrak{Q}_i$ ne le soit. Désignons par z_i un générateur de $\mathfrak{Q}_i$. Les complexes z_i^p et $x + \zeta^i y$ engendrent le même idéal, ils sont donc associés ; il existe une unité u_i telle que

$$u_i z_i^p = x + \zeta^i y$$

et en particulier $z_1 = u(x + \zeta y)$. On sait qu'il est possible d'écrire u_1 sous la forme du produit d'une unité réelle ρ par une racine de l'unité ζ^r. Soit a un entier rationnel tel que $z_1^p \equiv a \pmod p$:

$$x + \zeta y = \rho\zeta^r z_1^p \equiv \zeta^r a \pmod p$$
$$x + \zeta^{-1} y = \rho\zeta^{-r} \bar{z}_1^p \equiv \zeta^{-r} a \pmod p$$

d'où l'on tire la congruence

$$\zeta^{-r}x + \zeta^{-1}y \equiv \zeta^{r}x + \zeta^{1}y \pmod{p}.$$

qui ne peut être réalisée sans que x et y ne soient divisible par p. □

Comme l'avait annoncé Lamé, la démonstration du deuxième cas de l'hypothèse de Fermat se fait par des arguments analogue mais nécessite aussi une descente infinie, voir [9, 11].

22. Les nombres de Bernoulli

Depuis que j'enseigne l'algorithmique, j'ai pu me rendre compte que les étudiants de premier et second cycle manquent de bases solides, notamment en matière de formules sommatoires. La légende raconte que Gauss enfant savait calculer la somme des n premiers entiers, 200 ans après lui, trop d'étudiants des classes scientifiques supérieures ne savent pas restituer correctement la formule :

$$0 + 1 + 2 + \cdots + \cdots + n - 1 = (n-1)n/2 = \frac{1}{2}n^2 - \frac{1}{2}n$$

Que se passe-t-il pour les sommes analogues avec des exposants supérieurs ? Il est assez facile de voir que la somme des puissances p-ème des n premiers entiers est grosso modo (une manière décontractée de parler d'équivalent !) égale à $\frac{1}{p+1}n^{p+1}$. D'après le premier volume de l'encyclopédie mathématique soviétique dirigée par Vinogradov, le mathématicien Jacob Bernoulli (1654–1705) serait le premier à avoir proposer une formule générale :

$$\sum_{k=0}^{n-1} k^p = \frac{1}{p+1}\sum_{i=0}^{p} C_p^i B_i n^{p+1-i}$$

où les B_i sont des nombres rationnels, les nombres de Bernoulli. Une formule publiée en 1713 par Johann Bernoulli (1676–1748), le frère de Jacob. Les nombres de Bernoulli sont liés au développement de la série entière :

$$\frac{z}{e^z - 1} = \sum_{k=0}^{\infty} B_k \frac{z^k}{k!}$$

Une formule relativement élégante qui laisse présager quelques applications remarquables. Les termes de rangs impairs > 1 sont tous nuls, la table ci-dessous donne un échantillon des valeurs de $(-1)^{n+1}B_{2n}$:

Un nombre premier p est dit régulier s'il ne divise pas le nombre de classes d'idéaux de l'anneau $\mathbf{A}_p$. Le théorème de la section précédente montre l'importance de cette notion puisque le théorème de Fermat est vrai pour tous les nombres premiers réguliers. La proposition suivante permet de décider du caractère régulier d'un premier.

Proposition 8 (Kummer)**.** *Le nombre premier p est régulier si et seulement s'il ne divise aucun des numérateurs des nombres de Bernoulli B_k, pour $k = 2$, 4, 6,. . ., $p - 3$.*

Démonstration. Il faut écrire une formule pour le nombre de classes d'un corps cyclotomique et c'est bien loin d'être trivial ! □

TAB. 1. Quelques nombres de Bernoulli $(-1)^{n+1}B_{2n}$

n	numérateur	dénominateur	n	numérateur	dénominateur
0	1	1	10	1746711	330
1	1	6	11	854513	138
2	1	30	12	236364091	2730
3	1	42	13	8553103	6
4	1	30	14	23749461029	870
5	5	66	15	8615841276005	14322
6	691	2730	16	7709321041217	610
7	7	6	17	2577687858367	6
8	3617	510	18	26315271553053477373	1919190
9	43867	798	19	2 92999 3913841559	6

Par exemple, la factorisation de B_{32} :

$$7709321041217 = 37 \times 683 \times 305065927$$

montre que 37 est irrégulier. Les autres premiers inférieurs à 100 sont réguliers sauf deux : 59, 67.

23. Une période de doute

Entre Kummer et le début du XX^e, l'arithmétique et la géométrie font des progrès considérables : théorie de Galois, anneaux de Dedekind, corps de classes de Hilbert, variétés algébriques. Les principaux continuateurs de Kummer : Coppersmith, Fürtwangler, Granville, Mirimanoff, Monagan, Tanner, Vandiver, Wagstaff, Wiefrich. Les méthodes d'attaques du monstre s'améliorent et la conjecture de Fermat est vérifiée pour un très grand nombre de premiers. En 1993, le théorème est complètement prouvé pour tous les entiers inférieurs à 4.000.000, et le premier cas est vérifié jusqu'à $7.568\,10^{17}$! En 1995, Jensen prouve l'existence d'une infinité d'irréguliers ce qui limite l'approche de Kummer.

Le cas des nombres irréguliers reste ouverts. Les académies scientifiques vont recevoir leurs lots de démonstrations fausses. Pour ma part, j'ai fait connaissance avec ce problème quand j'étais lycéen, en classe de première ou de terminale. Comme bien d'autres, j'ai tenté ma chance et je me suis perdu à plusieurs reprises dans des récurrences alambiquées !

Les progrès enregistrés par les logiciens dans les années trente vont faire changer le statut de l'hypothèse de Fermat. Le logicien Kürt Gödel (1906–1978) répond négativement aux problèmes de décidabilité et de complétude proposés quelques années auparavant par David Hilbert (1862–1943). Gödel démontre l'indécidabilité de l'univers arithmétique ce qui signifie que certaines assertions arithmétiques sont indémontrables à partir de l'axiomatique universellement admise par tous. La preuve n'est pas effective mais rien ne s'oppose à ce que l'énoncé de Fermat fasse partie de ces monstres logiques.

Finalement, les vaines tentatives des amateurs, des professionnels, des génies et des fous sont autant d'arguments pour plaider en faveur de l'indécidabilité de la proposition de Fermat.

Théorème 8 (Zinoviev, 1977)**.** *Le théorème de Fermat est une hypothèse indécidable. indémontrable.*

Démonstration. La preuve donnée par Zinoviev est fausse. □

Quoiqu'il en soit, travailler sur le théorème de Fermat est considéré comme une affaire risquée et les arithméticiens vont s'occuper à d'autres questions concernant la masse des résultats induits par la théorie des nombres : théorie de Galois, corps de fonctions, théorie du corps de classes etc...

24. Galoiseries

Malgré ses brillants succès sur la résolution des équations algébriques, l'école italienne du XVI^e reste impuissante devant l'équation du cinquième degré. Paolo Ruffini (1765–1822) fût le premier à comprendre la nature de l'obstruction en expliquant pourquoi il était impossible de résoudre certaine équations algébriques du cinquième degré sans plus d'outils que les opérations usuelles et les extractions de radicaux.

Pour travailler sur cette question, Lagrange invente la notion de groupe et de fonctions invariantes qui seront exploitées par deux des trois étoiles filantes du monde mathématique du début du XIX^e : le norvégien Niels Abel (1802–1829) et le parisien Évariste Galois (1811–1832).

Théorème 9 (Abel)**.** *Une équation algébrique de degré supérieur à cinq n'est pas résoluble toujours résoluble par radicaux.*

La théorie de Galois est omniprésente en arithmétique car elle explique les mécanismes des extensions algébriques. Un élément du corps des nombres complexes est dit algébrique sur $\mathbf{Q}$ s'il est racine d'un polynôme non-nul à coefficients rationnels. Pour un polynôme irréductible f de degré n, on sait construire une extension (corps de décomposition) algébrique minimale K de $\mathbf{Q}$ qui contient toutes les racines de f. L'ensemble des automorphismes de L forme un groupe, c'est le groupe de Galois du polynôme f ou bien celui de l'extension $\mathrm{Gal}(K)$.

Il est important de remarquer que la notion de racine d'un polynôme est une notion ambiguë. Il n'existe pas de procéder fiable permettant de privilégier une racine plutôt qu'une autre. En quelques sorte, le groupe de Galois d'une extension est ce qui reste lorsqu'on a tout oublié. Un des buts de cette théorie est de tirer des informations sur la nature des racines d'une équation par la seule observation de son groupe de Galois. Un point de vue qui implique le développement de la théorie des groupes.

Théorème 10. *Une équation algébrique de est résoluble par radicaux si et seulement si son groupe de Galois est résoluble.*

25. Groupe et représentation

Un groupe G est un ensemble muni d'une loi de composition interne associative, admettant un élément neutre e tel que chaque élément admet un symétrique.

$$\forall x \in G \quad \exists y \in G, \qquad x * y = y * x = e$$

La puissance n-ème de $x \in G$ est l'élément x^n qu'on obtient en itérant n fois le produit de x par lui même. On définit l'ordre de x comme étant le plus petit entier non nul n tel que $x^n = e$. La proposition qui suit nous rappelle la présence de Lagrange comme fondateur de ces notions

Proposition 9 (Lagrange). *Dans un groupe fini l'ordre d'un élément divise le cardinal du groupe.*

Bien entendu tous les éléments ne sont pas d'ordre fini. Dans le cas d'un groupe abélien (commutatif), on introduit la notion de torsion et de rang qui permettent de voir G comme un produit direct :

$$G \sim \mathrm{tor}(G) \times \mathbf{Z}^r$$

La notion d'endomorphismes d'espaces vectoriels, génère un lot de « groupes classiques » décrits par Léonard Eugène Dickson (1874–1954). Les matrices carrées d'ordre deux à coefficients dans un anneau A forme un anneau dont le produit est :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} a\alpha+b\gamma & a\beta+b\delta \\ c\alpha+d\gamma & c\gamma+d\delta \end{pmatrix} \tag{5}$$

On définit le déterminant de $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ par $\det(X) = ad - bc$, c'est une application multiplicative i.e. $\det(XY) = \det(X)\det(X)$. Les matrices dont le déterminant est un inversible de A forment un groupe, le groupe linéaire $\mathrm{GL}_2(A)$ dont les éléments de déterminants 1 constituent le sous-groupe spéciale linéaire $\mathrm{SL}_2(A)$.

Exercice 11. *Quel est l'ordre de* $\mathrm{GL}_2(\mathbf{F}_p)$.

Exercice 12. *Quel est l'ordre de* $\mathrm{SL}_2(\mathbf{F}_p)$.

26. Le cinquième élément

Un des principes de base de la méthodologie scientifique est de comprendre la nature de certains objets en les faisant agir sur d'autres. C'est ainsi que d'une manière générale, on apprend plus de chose sur un ensemble de points par l'étude des fonctions définie sur cet ensemble comme par exemple en analyse fonctionnelle ou encore en géométrie différentielle. Des nombres, nous déduisons quatre opérations. Parmi les actions les plus élémentaires, nous retenons la translation $z \mapsto z+1$ et l'inversion $z \mapsto \frac{1}{z}$. L'objectif de la théorie modulaire est de comprendre les nombres au travers de ces deux actions élémentaires. D'après une boutade de Eichler, en arithmétique, il y aurait cinq opérations : l'addition, la soustraction, la multiplication, la division et les fonctions modulaires.

Pour des raisons techniques de cette théorie, il est préférable d'observer au travers de transformations légèrement modifiées : $S\colon z \mapsto -\frac{1}{z}$ et $T\colon z \mapsto z + 1$. Ces deux éléments engendrent un groupe isomorphe aux matrices carrées à coefficients entiers de déterminant 1, le groupe spécial linéaire $\mathrm{SL}_2(\mathbf{Z})$. Un élément g de ce groupe s'écrit $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et l'action de g sur z est $g.z = \frac{az+b}{cz+d}$. Le lecteur curieux d'approfondir ses connaissances sur le sujet est renvoyé vers le petit cours d'arithmétique de Jean-Pierre Serre, un des spécialistes de ces questions.

Le groupe modulaire agit sur le demi-plan de Poincaré $\mathfrak{H} = \{z \in \mathbf{C} \mid \mathrm{Im}(z) > 0\}$. Une fonction faiblement modulaire de poids $2k$ est une fonction complexe f méromorphe sur $\mathfrak{H}$ vérifiant les relations :

$$\forall z \in \mathfrak{H} \qquad f(z+1) = f(z), \quad \text{et} \quad f(-1/z) = z^{2k} f(z).$$

Le demi-plan plan de Poincaré s'envoie sur le disque unité privé de son origine par $z \mapsto q = e^{2i\pi z}$, de l'invariance par T d'une fonction modulaire, on déduit une fonction $\tilde{f}$ méromorphe sur le disque privé de l'origine telle que $\tilde{f}(q) = f(e^{2i\pi z})$. Lorsque $\tilde{f}$ est méromorphe en 0, on dit que f est une fonction modulaire. On dit que f est une forme modulaire si $\tilde{f}$ est partout holomorphe sur le disque et enfin on dit que la forme f est parabolique ou cuspidale si $\tilde{f}(0) = 0$. Plus généralement, on introduit les formes modulaires de niveau N par une définition analogue en remplaçant le groupe moduaire par le groupe $\Gamma_0(N)$ formé des matrices carrées à coefficients entiers $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ de déterminant 1 tel que $c \equiv 0 \mod N$. Une forme modulaire de niveau N f vérifie $f(\frac{az+b}{cz+d}) = (cz+d)^2 f(z)$ pour tout a,b, c, d tels que $ad - bc = 1$ et $c \equiv 0 \mod N$. Le produit infini :

$$q \prod_{n=1}^{\infty} (1-q^n)^2 (1-q^{11n})^2 = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - \dots$$

définit une forme modulaire de niveau 11.

27. Objets elliptiques

Les textes mathématiques sont émaillés de quelques qualificatifs déconcertants. On devine bien l'existence d'un lien entre les ellipses et les courbes elliptiques mais lequel ? Nous restons perplexes quand le narrateur du film présenté à ces journées de la sciences nous dit qu'il ne faut pas confondre une ellipse et une courbe elliptique puisque ces dernières sont des surfaces plus proche du beignet que du cercle. Pour comprendre cette terminologie, il faut remonter à l'époque de Keppler (1571–1630) et Galiée (1564–1642). L'exposé révolutionnaire du second et les lois du premier en conjonction avec la découverte du calcul intégral conduisent les mathématiciens à chercher une formule pour donner la longueur d'un arc elliptique. Le premier a s'engager sur cette question est l'anglais Wallis (1616–1703) un contemporain de Fermat. Il est suivi de Newton (1643–1727), puis de Fagnano (1682–1766) et de l'inévitable Léonard Euler. Dans ce contexte apparaissent des fonctions elliptiques, des intégrales elliptiques et des courbes elliptiques. Peu à peu, les mathématiciens se sont intéressés à ces nouveaux objets et le lien génétique à l'ellipse ne tient plus que par le fil terminologique ! Dans ces calculs d'arcs elliptiques apparaissent des radicaux de la forme $\sqrt{f(t)}$ où $f(X)$ est un polynôme de degré trois. Au polynôme $f(X)$ est associée une courbe algébrique constituée des points (x, y) à coordonnées complexes vérifiant l'équation :

$$Y^2 = f(X),$$

et on parle de courbe elliptique lorsque $f(X)$ est sans facteur double. Plus généralement, si K est un corps arbitraire, et si $f(X)$ est un polynôme à coefficients dans K, sans racine multiple dans la clôture algébrique L de K, alors l'ensemble des solutions $(x, y) \in L^2$ est une courbe elliptique définie sur K.

28. Loi de groupe

Les courbes elliptiques jouïssent de nombreuses propriétés remarquables. Principalement, une extension du théorème de Bézout montre que l'intersection d'une droite quelconque et d'une courbe elliptique est invariablement composée de trois points.

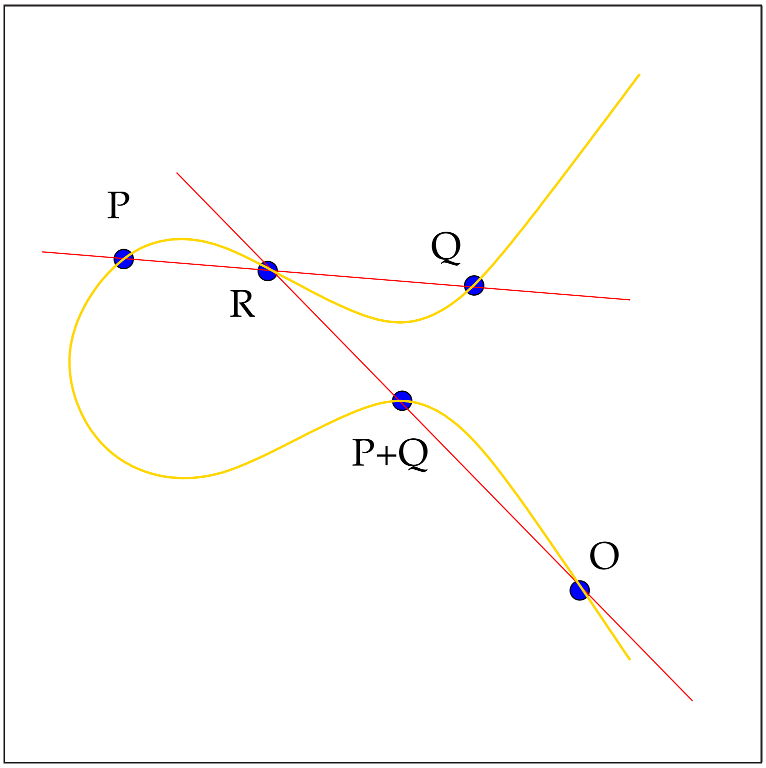

FIG. 2. Loi de groupe

Considérons E une courbe elliptique et O un point de E. On peut munir E d'une structure de groupe abélien telle que trois points alignés P, Q et R satisfont à la relation :

$$P + Q + R = O$$

Géométriquement, on obtient la somme de deux points distincts P et Q en procédant comme ci-après. La droite (P, Q) coupe E en un point X tel que $P + Q + X = O$ et donc la somme $P + Q$ est égale à l'intersection de E et la droite (X, O). Cette loi est clairement commutative, l'associativité est plus délicate à établir.

Exercice 13 (Duplication)**.** *Une définition analogue permet de calculer* $2P$ *en passant par les tangentes. Déterminez graphiquement tous les points d'ordre* 2 *de la courbe.*

29. Les beignets

Liouville, Eisenstein (1823–1852) et Weierstrass (1815–1897) tous contemporains de Kummer travaillent sur les fonctions elliptiques. Ils utilisent la toute nouvelle théorie des résidus de Cauchy pour dégager les propriétés cachées de ces fonctions. À cette période, l'université de Berlin réunit des mathématiciens remarquables : l'arithméticien Kummer, le géomètre Kronecker et l'analyste Weierstrass. Leurs travaux préparent la le terrain pour la démonstration du théorème de Fermat qui prend sa forme finale un siècle et demi plus tard. Bien entendu, ces trois hommes, trois amis aussi, sont bien loin de l'imaginer.

Une fonction elliptique est une fonction méromorphe doublement périodique. Une fonction elliptique f de périodes $\{u, v\}$ vérifie

$$\forall z \in \mathbf{C}, \quad f(z+u) = f(z+v) = f(z) \tag{6}$$

On suppose que l'indépendance linéaire sur $\mathbf{R}$ des vecteurs u et v. L'ensemble $\Lambda = \{mu + nv \mid m, n \in \mathbf{Z}\}$ s'appelle un réseau, c'est un sous-groupe discret de $\mathbf{C}$ et la théorie des groupes permet de construire un groupe quotient $\mathbf{C}/\Lambda$. L'ensemble des fonctions elliptiques du réseau Λ est un corps $\mathbf{C}(\Lambda)$ contenant les constantes. Weiserstrass utilise la théorie des fonctions analytiques pour exhiber un représentants moins trivial, c'est la fameuse fonction « P » de Weierstrass :

$$\wp(z) = -\frac{1}{z^2} + \sum_{\omega \in \Lambda} \left(\frac{1}{(z-\omega)^2} - \frac{1}{w^2}\right)$$

Une série qui converge uniformément sur tout compact inclus dans $\mathbf{C} - \Lambda$ comme on peut s'en rendre compte en faisant intervenir les séries d'Eisenstein :

$$G_{2k} = \sum_{\omega \in \Lambda} \frac{1}{w^{2k}}$$

qui convergent normalement sur le même domaine pour tous les entiers positifs. L'ensemble des fonctions elliptiques est fermé pour la dérivation, en particulier :

$$\wp'(z) = -2 \sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^3}$$

est une fonction elliptique.

Théorème 11 (Liouville)**.** *Le corps des fonctions elliptiques est engendré par la fonction de Weierstrass et sa dérivée. Plus précisément,*

$$(\wp')^2 = 4\wp^3 - 60G_4\wp - +140G_6$$

Démonstration. Pour le materiel de cette section, voir [10]. □

L'application $\phi\colon \mathbf{C}/\Lambda \longrightarrow E$ qui envoie z sur $\big(\wp'(z), \wp(z)\big)$ est bijective, c'est un isomorphisme de groupe de Lie du nom du mathématicien norvégien Marius Lie (1842–1899). Un tel isomorphisme permet d'identifier une courbe elliptique à un quotient $\mathbf{C}/\Lambda$ c'est-à-dire un tore, un « beignet ».

30. Discriminant et conducteur

Une courbe elliptique est à la fois une courbe algébrique (une variété de dimension 1) et une variété abélienne (munie d'une structure de groupe). L'ensemble des courbes elliptiques sur un corps K est paramétré par l'application qui envoie le pentuplet $(a_1, a_2, a_3, a_4, a_6) \in K^5$ sur une équation de Weierstrass :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{7}$$

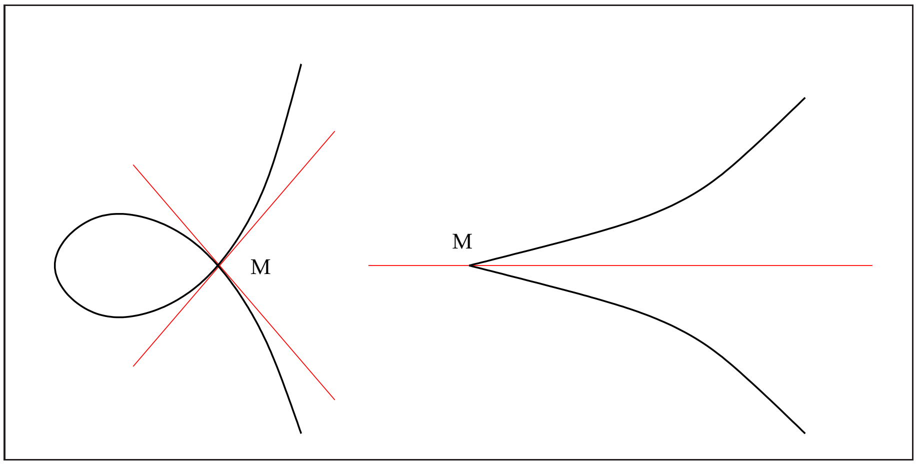

FIG. 3. Loi de groupe

Les courbes elliptiques obtenues par cette paramétrisation correspondent aux courbes non singulières i.e. sans point double ni point de rebroussement. Rappelons qu'un point $M(x,y)$ de la courbe d'équation (7) est une singularité s'il annule les équations dérivées :

$$y + a_1 x + a_3 = 0$$
$$a_1 y = 3x^2 + 2a_2 x + a_4$$

Dans ce cas, la courbe est dite singulière en M. La singularité est de type multiplicatif si la courbe possède deux tangentes et multiplicative sinon.

Le discriminant de la courbe (7) est la quantité :

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6$$

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, & b_4 &= 2a_4 + a_1 a_3 \\ b_6 &= a_3^2 + 4a_6, & b_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2. \end{aligned}$$

Les changements de variables permettent de définir une notion d'isomorphisme entre les courbes elliptiques. Le discriminant n'est pas un invariant pour cette notion mais une courbe elliptique définie sur $\mathbf{Q}$ possède un modèle minimal. Le modèle minimal d'une courbe elliptique définie sur E est une courbe à coefficients entiers, de discriminant minimal parmi celles lui sont isomorphe.

Une équation à coefficients entiers peut être réduite modulo n'importe quel entier de sorte à obtenir une courbe définie sur l'anneau $\mathbf{Z}/n\mathbf{Z}$. En particulier, la réduction modulo p d'une courbe elliptique donne une courbe de degré trois définie sur le corps fini $\mathbf{F}_p$. On parle de bonne réduction lorsque la courbe réduite demeure elliptique sur $\mathbf{F}_p$ ce qui est équivalent à dire que p ne divise pas le discriminant de la courbe d'origine.

31. Hypothèse de Riemann

Dans ses travaux sur la distribution des nombres premiers, Euler n'hésite pas à utiliser l'identité

$$\sum_{n\geq 1}\frac{1}{n} = \prod_{p\,\text{premier}}(1-\frac{1}{p})^{-1} \tag{8}$$

pour deviner la distribution des nombres premiers à savoir que le nombre de premiers inférieurs à n, en général noté $\pi(n)$, est équivalent à $\frac{n}{\log(n)}$. Une formule qu'il a probablement devinée par l'expérimentation numérique c'est-à-dire en faisant une table des valeurs de $\pi(n)$, Gauss lui donnera raison en faisant une preuve rigoureuse. L'identité (8) est incorrecte puisque le membre de gauche ne converge pas. Pour remédier aux questions de convergences, Bernhard Riemann (1826–1866) introduit sa fameuse fonction « zêta »

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

où les $\zeta_p(s) = (1-\frac{1}{p^s})^{-1} = \sum_{0\leq k} p^{-ks}$. La fonction ζ converge pour tout les complexes s tels que $\Re(z) > 1$. On remarque que les ζ_p vérifient des égalités fonctionnelles $\zeta_p(s) = -p^s\zeta_p(s)$ qui suggèrent de poser $\Lambda_p(s) := p^{-s/2}\zeta_p(s)$ de sorte que $\Lambda_p(s) = -\Lambda_p(-s)$. La fonction ζ vérifie une égalité similaire.

Théorème 12 (Riemann, 1859)**.** *La fonction ζ de Riemann définie par la série (**??**) pour tous les nombres complexes de partie réelle supérieure à 1 se prolonge analytiquement sur $\mathbf{C}$ en une fonction méromorphe dans tout le plan complexe avec un pôle unique en 1 de résidus 1. De plus la fonction $\Lambda(s) := \pi^{s/2}\Gamma(s/2)\zeta(s)$ vérifie l'équation fonctionnelle $\Lambda(s) = \Lambda(1-s)$.*

Dans l'énoncé du théorème, $s \mapsto \Gamma(s) = \int_0^\infty e^{-t}t^s\frac{\mathrm{d}t}{t}$ est désigne la fonction gamma d'Euler. Notez bien que cette fonction est beaucoup plus naturelle qu'elle ne paraît puisque construite à partir d'objets fondamentaux : mesure invariante, homomorphismes additif et multiplicatif. La fonction gamma vérifie $\Gamma(s+1) = s\Gamma(s)$. Les entiers pairs négatifs annulent la fonction zêta de Riemann, l'étude expérimentale de la distribution des nombres premiers suggère la formidable conjecture :

Conjecture 3 (Hypothèse de Riemann)**.** *Les zéros non triviaux de la fonction ζ se situent sur l'axe d'équation $\Re(s) = \frac{1}{2}$.*

L'autichien Emile Artin (1898–1962) suggère une généralisation de la construction de Euler-Riemann aux anneaux de Dedekind. Dans un anneau de Dedekind A, pour tout idéal non nul $\mathfrak{I}$, le quotient $A/\mathfrak{I}$ est de cardinal fini, le nombre des éléments de $A/\mathfrak{I}$ s'appelle la norme de $\mathfrak{I}$, on le note $N(\mathfrak{I})$. La norme est multiplicative, et l'unicité de la décomposution en produit d'idéaux premiers permet de décomposer la fonction ζ_A en un produit Eulérien.

$$\sum_{\mathfrak{I}\,\text{idéal}}\frac{1}{N(\mathfrak{I})^s} = \prod_{\mathfrak{P}\,\text{premier}}\frac{1}{1-N(\mathfrak{P})^{-s}} \tag{9}$$

La géométrie algébrique associe à une courbe elliptique E d'équation $Y^2 = f(X)$ sur un corps K, un anneau quotient $A := K[X,Y]/(Y^2 - f(X,Y))$. Aux idéaux premiers de A correspondent des points de E. Dans cette correspondance une point à l'infini est « oublié » par ma présentation affine des choses, quoiqu'il en soit, on définit alors la fonction :

$$\zeta_E(s) = \frac{1}{1-p^{-s}}\zeta_A(s),$$

où le terme $\frac{1}{1-p^{-s}}$ correspond au point à l'infini.

Théorème 13 (Artin)**.**

$$\zeta_E(s) = \frac{1-a(E)T+pT^2}{(1-T)(1-pT)}$$

où $T = \frac{1}{p}$ et $p - a(E) + 1$ désigne le nombre de points de E sur le corps $\mathbf{F}_p$.

On obtient comme corollaire que la fonction ζ_E vérifie l'hypothèse de Riemann ! Un résultat généralisé à toutes les courbes par Helmut Hasse (1898–1979) et André Weil (1906–1998) et qui vaut pour les variétés de plus grandes dimensions d'aprés des travaux de Groetendick et Deligne des années soixante-dix.

32. Conjecture de Taniyama-Schimura-Weil

Soit E une courbe elliptique définie sur $\mathbf{Q}$ d'équation mimnimale $F(X,Y)=0$, on ne peut plus procéder comme dans la section précédente.

Exercice 14. *Pourquoi ?*

Pour chaque premier p, on note $\bar{E}_p$ la réduction de E en p et si elle est bonne on note $L_{\bar{E}}(s)$ le numérateur de la fonction zéta d'Artin.

(10)

$$L_p(s) = \begin{cases} L_{\bar{E}}(s) & E \text{ admet une bonne réduction en } p\,; \\ (1-p^{-s})^{-1} & E \text{ admet une réduction de multiplicative rationnelle}\,; \\ (1+p^{-s})^{-1} & E \text{ admet une réduction de multiplicative irrationnelle}\,; \\ 1 & E \text{ admet une réduction de additive.} \end{cases}$$

et on pose :

$$L_E(s) = \prod_p L_p(s)$$

Un théorème de Néron montre que L_E est bien définie i.e. ne dépend pas du modèle minimale de E. On sait définir le conducteur de E, un entier qui s'écrit :

$$N_E = \prod_{p\,\text{mult.}} p \times \prod_{p\,\text{add.}} p^{2+\delta_p} \tag{11}$$

où δ_p est un entier nul dès que $p > 3$. Pour obtenir l'équation fonctionnelle de L_E, on introduit la fonction

$$\Lambda_E(s) := \left(\frac{\sqrt{N_E}}{2\pi}\right)^s \Lambda(s) L_E(s)$$

qui vérifie

$$\Lambda_E(s) = \pm\Lambda_E(2-s)$$

Tab. 2. Nombre de points de $y^2 = x^3 - x^2 + 1/4$.

p	3	5	7	11	13	17
$a(b)$	-1	1	-2	-	4	-2

où les a_p sont tous donnés par

$$\sharp E(\mathbf{F}_p) = 1 - a_p + p.$$

Nous avons commencé cette section par une conjecture fondamentale qui apparaît dans la liste des sept problèmes du millénaire i.e. la version mathématique du jeu « Qui veut gagner des milions ? ». Chacun son truc ! Profitons de l'occasion pour en signaler une autre qui relève des courbes elliptiques, la conjecture de Birch-Swinnerton-Dyer qui affirme que le rang du groupe de E est égal à l'ordre du pôle de $\Lambda_E(s)$ en $s = 1$.

$$\prod_{\substack{p \leq R \\ p \not| \Delta}} \frac{\sharp \bar{E}_p(\mathbf{F}_p)}{p} \sim K(\log R)^r$$

33. conjecture de Taniyama-Schimura-Weil

Écrivons le développement de $L_E(s)$ sous la forme d'une série de Dirichlet, c'est-à-dire :

$$L_E(s) = \sum_{n \geq 1} a_n n^{-s}$$

qui permet de définir une certaine fonction f_E sur le demi-plan de Poincaré $\mathfrak{H}$ à valeurs dans $\mathbf{C}$ par

$$\tau \mapsto \sum_{n \geq 1} a_n q^n$$

où l'on a posé $q = e^{2i\pi\tau}$.

Conjecture 4 (Taniyama-Shimura-Weil)**.** *La fonction f_E est une forme modulaire parabolique, de niveau* $\mathrm{cond}(E)$ *et de poids* 2*. De plus,*

$$f_E\left(\frac{-1}{\mathrm{cond}(E)\tau}\right) = \pm \mathrm{cond}(E)\tau^2 f_E(\tau)$$

Considérons la courbe elliptique

$$y^2 = x^3 - x^2 + 1/4.$$

À la main, ou avec une machine, il est assez facile de compter le nombre de points de la réduction modulo p pour des petites valeurs de p. On écrit $\sharp E(\mathbf{F}_p) = p + a(p) + 1$, et la table (2) donne les valeurs de $a(p)$.

34. Représentation Galoisienne Elliptique

35. Représentation Galoisienne Modulaire

36. Les conjectures de Serre

On suppose que E est une courbe elliptique définie sur $\mathbf{Z}$. Le groupe de Galois de la clôture algébrique de $\mathbf{Q}$, traditionnellement noté $\mathrm{G}_{\mathbf{Q}}$ agit sur les points de E et sur le groupe des points de n-torsion $E[n]$. Nous savons que $E(\mathbf{C})$ est isomorphe à $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$. Le groupe $\mathrm{G}_{\mathbf{Q}}$ agit sur le plan projectif $P^2(\bar{\mathbf{Q}})$, sur $E(\bar{\mathbf{Q}})$ ainsi que sur chacun des les $E[n]$. En choisissant un isomorphisme de groupes entre $E[n]$ et $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$, on obtient une représentation Galoisienne modulo n de E :

$$\rho_{E,n} \colon \mathrm{G}_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z}).$$

Par ailleurs, les points de $E[n]$ sont dans un corps de nombres K et donc, pour chaque n, il existe une extension finie K telle que $\rho_{E,n}$ se factorise au travers de $\mathrm{Gal}(K/\mathbf{Q})$. Au début des années soixante-dix, Serre s'est posé deux questions fondamentales concernant ces deux types de représentations. Étant donné une représentation galoisienne continue modulo p et irréductible.

(1) Sous quelles hypothèses ρ provient d'une forme modulaire ?
(2) Dans l'affirmative, quel est le type (N, k, ϵ) minimal ?

Conjecture 5 (Serre, 1973)**.** *ρ provient d'une forme modulaire si et seulement si* $\det\big(\rho(c)\big) = -1$.

37. Intuition d'Hellegouarch

À la fin des années soixante, Yves Hellgouarch, particulièrement bien inspiré associe à un hypothétique triplet (a, b, c) solution de l'équation de Fermat $a^p + b^p = c^p$, une nouvelle équation de deux variables :

$$y^2 = x(x - a^p)(x - b^p).$$

Quelle idée étrange, non ? Les points du « plan » satisfaisant à cette équation définissent une courbe algébrique.

38. Une idée brillante de Frey

39. La conjecture epsilon

40. Le théorème de Wiles

41. Wiles ⇒ Fermat

42. Epilogue

L'anneau des polynômes à coefficients $\mathbf{Z}[X]$ partage beaucoup de propriétés avec celui des entiers relatifs. L'hypothèse de Fermat étant vérifiée dans $\mathbf{Z}$, elle l'est a fortiori dans $\mathbf{Z}[X]$. Nous allons en faire une démonstration spécifique qui ne sera pas sans conséquence. Dans la suite $\deg(A)$ désigne le degré du polynôme A, et moins usuellement $\rho(A)$ désigne le degré du radical de A, c'est aussi le nombre de racines distincts de A dans une clôture algébrique.

Théorème 14 (Mason)**.** *Soient A, B et C trois polynômes deux à deux premiers entre eux tels que $A + B = C$.*

$$\max\{\deg(A), \deg(B), \deg(C)\} \leq \rho(ABC) - 1$$

Démonstration. □

43. Thanks

Cette note s'inscrit dans un programme de présentation des activités du Groupe de Recherche en Informatique et Mathématiques. Une petite conférence, des affiches et ce document. Pour les collaborations diverses et variées, tous mes sincères remerciements à destination de Michel Dufour pour ses traductions, Pierrick Gaudin pour l'affiche, Pascal Véron et Patrice Rabizzoni pour la bande déssinée, Jacques Wolfmann pour la prise en charge de la conférence, Jean-Pierre Zanotti pour les problèmes de mises en pages, les internautes `fr.sci.maths`, et en particulier Antoine Chambert-Loir et Vincent Michel pour la cassette.

Until yesterday I had no definite intention of killing myself. ... I don't quite understand it myself, but it is not the result of a particular incident, nor of a specific matter.

About a month later the girl who he was planning to marry also committed suicide.

Références

[1] Ebbinghaus H.-D. & als. *Les Nombres...* Vuibert, 1998.

[2] Gauss C. F. *Disquisitiones Arithmeticae*, volume section VII. 1807.

[3] Itard J. *Les nombres premiers*, volume x des *Que sais-je ?* PUF, 1975.

[4] Itard J. *Les nombres premiers*, volume 1093 des *Que sais-je ?* PUF, 1963.

[5] Samuel P. *Théorie Algébrique des Nombres.* Hermann, 1971.

[6] Dahan-Dalmedico A., Peiffer J. *Une histoire des mathématiques, routes et dédales.* Éditions du seuil (collection Points sciences), 1986.

[7] Hindry, Schoof, Edixhoven, Cohen, Terjanian *Dossier Fermat-Wiles* Gazette des mathématiciens, numéro 66, 1995.

[8] Coldstein, Ferr'eol, Cohen, Terjanian, Balazard, Hellegouarch *Grand théorème de Fermat 1641–1994*† quadrature, été 1995.

[9] Edwrads H. M. *Fermat's Last Theorem : A genetic Introduction to Algebraic Number Theory.* Graduate Texts in Mathematics (50) Springer-Verlag, 1977.

[10] Silverman J. H. *The Arithmetic of Elliptic Curves* Graduate Texts in Mathematics (106) Springer-Verlag, 1986.

[11] Washington L. C. *Introduction to cyclotomic fields* Graduate Texts in Mathematics (83) Springer-Verlag, 1982.

[12] Ribet K. A. *Galois representations and modular forms* Bulletin of the AMS (32) n. 4 pages 375–402, 1995.

[13] Lang S. *Algebra* Addison Wesley, 1993.

[14] Simon Singh et John Lynch *The Last Fermat Theorem (script du film)* `www.bbc.co.uk/horizon/fermat.shtml`

[15] School of Mathematics and Statistics of St-Andrew University *The MacTutor History of Mathematics archive* `www-groups.dcs.st-andrews.ac.uk/`

[16] William Stein *Hecke Algebras and Modular Forms : notes derived from Ribet's 1996 Berkeley grad. course* `http ://modular.fas.harvard.edu/MF.html`