Que cherche un mathématicien ?

Quelques exemples,

de l'Antiquité aux problèmes du Millenium.

Daniel PERRIN

Table des matières

1 Première époque : l'Antiquité **3**
1.1 Les nombres premiers 3
1.2 Les équations algébriques 5
1.3 Les équations diophantiennes 6
1.4 Les constructions à la règle et au compas 8

2 La période intermédiaire : de la Renaissance à 1900 **11**
2.1 Les nombres premiers 11
2.2 Les équations algébriques 15
2.3 Les équations diophantiennes 17
2.4 Les constructions 20

3 L'époque actuelle : 1900-2022 **22**
3.1 Les problèmes de Hilbert 22
3.2 Le vingtième siècle 23
3.3 Les sept problèmes du millenium 24
3.4 Le point sur deux autres conjectures 25
3.5 Bilan des quatre thèmes 25
3.6 D'autres sources de problèmes pour les mathématiciens 26
3.7 Et les applications ? 26
3.8 Quelques pistes de réflexion 26

Ce texte est la rédaction d'une conférence faite au lycée Marcel Dassault de Rochefort le 3 février 2023.

Introduction

Quand on dit qu'on fait de la recherche en mathématiques, la réaction des interlocuteurs "grand public" est souvent : *Ah bon, il y a encore quelque chose à trouver en maths ?*

Pourtant, oui, il y a beaucoup de questions sans réponses en mathématiques et la recherche y est très active : on dit couramment qu'il s'est fait plus de mathématiques nouvelles depuis 1945 que de l'origine des temps à 1945. Ainsi, à la bibliothèque de mathématiques de l'université à Orsay, il y a environ 400 revues qui publient chacune à peu près un millier de pages de mathématiques nouvelles chaque année. Pour donner un autre ordre de grandeur, le nombre de thèses de mathématiques soutenues en France entre 1800 et 1900 est de moins de 300, alors qu'il y en a eu plus de 500 en France pour la seule année 2020.

Soit, mais il reste une question : qu'est-ce qu'on cherche en mathématiques ? C'est une question difficile car l'énoncé de la plupart des problèmes actuels [1] est incompréhensible pour des lycéens, sauf dans certains domaines comme l'arithmétique. Je vais cependant tenter de répondre à cette question, en m'appuyant sur l'Histoire.

L'exposé est bâti autour de quatre thèmes : les nombres premiers, les équations algébriques, les équations diophantiennes [2] et les constructions à la règle et au compas.

Bien sûr, beaucoup d'autres choix sont possibles (en analyse [3], en probabilités, en statistiques, en logique, en topologie, etc.). Le choix ci-dessus est complètement subjectif, il correspond à mes préférences et à mes compétences.

Ces thèmes seront déclinés sur trois époques : l'Antiquité, une vaste époque intermédiaire (disons, de la Renaissance à 1900), et l'époque actuelle (à partir de 1900). Pour chacun de ces thèmes on dégagera une question centrale dans ce thème, qui nous servira de fil conducteur. On suivra cette question dans le temps en indiquant les réponses et les variations autour de cette question : des précisions, des modifications, des questions nouvelles. Les questions occupent une place essentielle dans la démarche scientifique comme le dit le philosophe Gaston Bachelard (1884-1962) :

1. Par exemple les fameux problèmes du Millenium, voir plus bas.
2. Ces mots seront expliqués plus loin.
3. Depuis l'invention du calcul infinitésimal par Newton et Leibniz, ce domaine est sans doute le plus important de toutes les mathématiques.

L'esprit scientifique nous interdit d'avoir une opinion ... sur des questions que nous ne savons pas formuler clairement. Avant tout, il faut savoir poser des problèmes. ... Pour un esprit scientifique, toute connaissance est une réponse à une question. S'il n'y a pas eu de question, il ne peut y avoir connaissance scientifique.

1 Première époque : l'Antiquité

1.1 Les nombres premiers

La notion de nombre premier est liée à celle de diviseur ou de multiple, qui apparaît dès que l'on mesure des grandeurs par des nombres [4]. Euclide (Alexandrie, 300 avant J.-C. ?) définit ces notions au début du Livre V de ses *Éléments* :

Une grandeur est une **partie** [5] *d'une grandeur, la plus petite de la plus grande, quand elle mesure la plus grande.*

Et **multiple**, *la plus grande de la plus petite, quand elle est mesurée par la plus petite.*

Le mot *mesurer* doit être compris au sens : la plus grande est égale à un nombre entier de fois la plus petite. D'ailleurs, chez Euclide, les nombres sont représentés par des segments comme sur la figure ci-dessous :

FIGURE 1 – Le segment $[AB]$ "mesure" $[CD]$

Cela permet à Euclide de définir (Livre VII def. 12) : *Un nombre premier est celui qui est mesuré par une seule unité.* Il en établit nombre de propriétés (notamment le fameux "lemme d'Euclide"). La question que l'on peut considérer comme cruciale sur ce thème est la suivante :

(QP) Y a-t-il beaucoup de nombres premiers ?

Le premier résultat en ce sens est l'infinitude de l'ensemble des nombres premiers et il est prouvé par Euclide (Livre IX, proposition 20). Il est intéressant de citer l'énoncé et le début de la preuve d'Euclide :

4. Une autre raison de l'importance de la divisibilité tient à l'utilisation d'un système de calcul à base 60 chez les Babyloniens où les diviseurs de 60 sont techniquement essentiels.
5. Il faut comprendre ce mot comme *diviseur*.

Les nombres premiers sont plus nombreux que toute multitude de nombres premiers proposée.

Voici le début de la preuve :

Soient les nombres premiers proposés A, B, C. Je dis que les nombres premiers sont plus nombreux que A, B, C. En effet, que soit pris le plus petit [nombre] mesuré par A, B, C, et que ce soit DE et que l'unité DF soit ajoutée à DE. Alors ou bien EF est premier ou bien non. D'abord qu'il soit premier ; donc sont trouvés les nombres premiers A, B, C, EF, plus nombreux que A, B, C. ...

Deux remarques :

1) On notera que la multitude d'Euclide est modeste : trois nombres A, B, C !

2) On retrouve aussi l'aspect géométrique : les nombres en question sont représentés par des segments, avec un segment unité $[DF]$, etc.

Sinon, dans le principe, cette preuve est essentiellement celle que l'on donne encore aujourd'hui :

1.1 Proposition. *Il y a une infinité de nombres premiers.*

Démonstration. Sinon, ils seraient en nombre fini $p_1, \ldots, p_r$ ($p_1 = 2$, $p_2 = 3$, etc.) On considère $n = p_1 \cdots p_r + 1$. Il est > 2, donc admet [6] un facteur premier p qui ne peut être l'un des p_i (sinon il diviserait 1), c'est donc un nombre premier autre que les p_i, contrairement à l'hypothèse.

1.2 *Remarques.* 1) Attention, le nombre $n = p_1 \cdots p_r + 1$ n'est pas nécessairement premier, par exemple on a $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509$.

2) Pour prouver l'existence d'un facteur premier pour tout entier ≥ 2 on raisonne comme suit. On suppose que ce n'est pas vrai, de sorte que l'ensemble des contre-exemples est un ensemble non vide d'entiers naturels. Il admet donc un plus petit élément n (c'est une propriété de $\mathbf{N}$, généralement prise comme axiome [7]). Mais alors, ce n n'est pas premier (sinon ce ne serait pas un contre-exemple), donc il s'écrit $n = ab$ avec $a, b \geq 2$. Mais a et b sont plus petits que n, donc ce ne sont plus des contre-exemples et ils admettent des facteurs premiers, donc n aussi et c'est absurde.

6. Ce résultat, intuitivement naturel, est dans Euclide, Livre VII, prop. 32. Voir aussi la remarque ci-dessous.

7. Euclide dit : *... des nombres en quantité illimitée mesureraient le nombre A, dont chacun serait plus petit que le précédent ; ce qui est impossible dans les nombres.*

1.2 Les équations algébriques

Il s'agit d'équations de la forme $P(x) = 0$ où P est un polynôme :

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0.$$

Le premier cas (hormis le premier degré, connu des Égyptiens) est celui du degré 2. On rencontre un exemple de telle équation avec le problème babylonien suivant :

Trouver les dimensions d'un champ rectangulaire dont l'aire est 96 *et la somme des dimensions est* 20.

Dit en termes modernes, on cherche x, y tels que l'on ait $xy = 96 := P$ et $x + y = 20 := S$. On a donc $y = 20 - x$ que l'on reporte dans l'autre équation et on obtient $x^2 - 20x + 96 = x^2 - Sx + P = 0$, qui admet les racines entières 12 et 8. Bien entendu, ici on peut traiter le problème de manière arithmétique [8] (par exemple en faisant la liste des diviseurs de 96), mais il suffit de modifier légèrement les données (par exemple $S = 20$, $P = 95$) pour que cette méthode ne fonctionne plus [9] .

Sur les équations algébriques, la question principale est la suivante :

(QE) Comment résoudre une équation algébrique ?

Dans le cas de l'équation du second degré, les Babyloniens disposaient d'un algorithme de résolution, qui donnait aussi le cas de racines non entières. Voici un exemple : il s'agit du problème 1 de la tablette BM 13901 - 1 dans la traduction [10] de Thureau-Dangin (1936).

J'ai additionné [11] *la surface et le côté de mon carré : 45'.*

Traduction. Rappelons que l'unité est fractionnée en 60 minutes, de sorte que $45' = 3/4$. Ici, on cherche x (le côté du carré) tel que $x^2 + x = 45'$ (on reconnaît une équation $ax^2 + bx + c = 0$ avec $a = 1, b = 1, c = -3/4$).

Solution : Tu poseras 1, l'unité. Tu fractionneras en deux 1 : 30'. Tu croiseras 30' et 30' : 15'. Tu ajouteras 15' à 45' : 1. C'est le carré de 1. Tu soustrairas 30', que tu as croisé, de 1 : 30', le côté du carré.

En clair : L'unité est b, on la divise en deux : $30' = 1/2$ et on "croise", c'est-à-dire qu'on multiplie : $(\frac{b}{2})^2 = \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$; on ajoute le résultat à $-c = 45'$, on trouve 1 : $(\frac{b}{2})^2 - c = \frac{1}{4} + \frac{3}{4} = 1 = 1^2$, on en prend la racine

8. C'est donc aussi une équation diophantienne, voir ci-dessous.

9. Ici, les racines ne sont plus rationnelles, ce sont $10 + \sqrt{5}$ et $10 - \sqrt{5}$.

10. Pour une intéressante discussion sur ce thème on renvoie à l'article de Christine Proust `http://images.math.cnrs.fr/Mathematiques-en-Mesopotamie.html`.

11. On notera que les Babyloniens ajoutent des longueurs et des aires. Les Grecs n'auraient jamais fait ça !

à laquelle on retranche $\frac{b}{2}$: $x = -\frac{b}{2} + \sqrt{(\frac{b}{2})^2 - c} = -\frac{1}{2} + 1 = \frac{1}{2}$. Avec nos yeux actuels on reconnaît la formule donnant les racines de l'équation avec le discriminant !

1.3 Les équations diophantiennes

Il s'agit encore d'équations (le plus souvent polynomiales), mais dont on cherche la solution **en nombres entiers** [12]. Leur nom vient du mathématicien grec Diophante d'Alexandrie (II^e ou III^e siècle après J.-C. ?, on ne sait pratiquement rien sur sa vie) qui a étudié de telles équations.

1.3.1 L'équation de Pythagore

Voici un exemple étudié par Diophante : *trouver tous les triangles rectangles à côtés entiers*. En vertu du théorème de Pythagore, cela revient à trouver les entiers x, y, z tels que l'on ait $x^2 + y^2 = z^2$.

Sur les équations diophantiennes, la question cruciale est donc double :

(QD1) Comment trouver **des** solutions d'une équation diophantienne ?
(QD2) Comment être sûr d'avoir **toutes** les solutions ?

Bien sûr, la deuxième question est en général beaucoup plus difficile. Diophante, lui, trouve [13] essentiellement toutes les solutions de l'équation de Pythagore :

1.3 Proposition. *Soient x, y, z une solution de l'équation $x^2 + y^2 = z^2$ avec $x, y, z \in \mathbf{N}^*$. On suppose que les entiers x, y, z sont deux à deux premiers entre eux* [14]*. Alors, à permutation près de x et y, il existe des entiers a, b avec $0 < a < b$ tels que l'on ait : $x = b^2 - a^2$, $y = 2ab$ et $z = a^2 + b^2$.*

Démonstration. Ici, il est facile de trouver des solutions en raisonnant ainsi. Si l'on a $x^2 + y^2 = z^2$, on a $z^2 - x^2 = y^2$ et le point crucial – la recette miracle en arithmétique – c'est qu'on peut factoriser $z^2 - x^2 = (z - x)(z + x)$. Une idée très simple est alors de prendre pour $z - x$ et $z + x$ des carrés : $z - x = a^2$ et $z + x = b^2$ qui donneront $y = ab$. On obtient $z = \dfrac{a^2 + b^2}{2}$ et $x = \dfrac{b^2 - a^2}{2}$ et

12. Voire parfois rationnels.

13. Une solution bien connue des charpentiers ou des maçons est $3, 4, 5$ qui sert à vérifier que des angles sont droits.

14. Sinon, on obtient de nouvelles solutions en multipliant x, y, z par un même nombre.

le problème c'est que ces nombres ne sont pas nécessairement entiers. Mais il est facile d'en trouver en prenant $x = b^2 - a^2$ et $z = b^2 + a^2$ et on obtient $z^2 - x^2 = 4a^2b^2$, donc $y = 2ab$. On vérifie qu'on a ainsi trouvé des solutions de l'équation, par exemple avec $b = 2$ et $a = 1$ on retrouve la solution $3, 4, 5$, avec $b = 3$ et $a = 2$ on a $5, 12, 13$, etc.

Pour montrer qu'on a toutes les solutions il faut travailler un peu plus.

Comme les entiers x, y, z sont deux à deux premiers entre eux, l'un au plus d'entre eux est pair. Il y en a nécessairement un qui est pair (car la somme ou la différence de deux impairs est paire). De plus, ce ne peut être z car si x, y sont impairs, on a une contradiction en raisonnant "modulo 4", c'est-à-dire en regardant les restes dans la division de x^2, y^2 et z^2 par 4. En effet, ce reste vaut 1 pour le carré d'un impair donc celui de $x^2 + y^2$ serait égal à 2, or le reste d'un carré pair (ici z^2) est nul.

Quitte à échanger x et y on peut donc supposer x, z impairs et y pair. On écrit alors l'équation sous la forme $z^2 - x^2 = y^2$ et on factorise $z^2 - x^2 = (z + x)(z - x) = y^2$. Si p est un facteur premier impair de y, il divise $z - x$ ou $z + x$, mais pas les deux, sinon il diviserait $(z + x) + (z - x) = 2z$ et $(z + x) - (z - x) = 2x$, donc diviserait aussi x et z, contrairement à l'hypothèse. Les facteurs impairs de y se répartissent donc en deux nombres a et b, l'un divisant seulement $z - x$ et l'autre seulement $z + x$ et comme y est au carré, cela signifie que l'on a $z + x = 2^\alpha b^2$ et $z - x = 2^\beta a^2$. De plus, on voit aussi que l'un des nombres α, β vaut 1 et que l'autre est impair égal à $2k + 1$ et on peut faire rentrer 2^{2k} dans le carré correspondant. En définitive, on a bien $z + x = 2b^2$ et $z - x = 2a^2$ et on retrouve la solution annoncée.

1.3.2 L'épitaphe de Diophante

Voici une autre équation diophantienne, qui est l'épitaphe de Diophante [15]. C'est une simple équation du premier degré :

Passant, sous ce tombeau repose Diophante.
Ces quelques vers tracés par une main savante
Vont te faire connaître à quel âge il est mort.
Des jours assez nombreux que lui compta le sort,
Le sixième marqua le temps de son enfance ;
Le douzième fut pris par son adolescence.
Des sept parts de sa vie, une encore s'écoula,
Puis s'étant marié, sa femme lui donna
Cinq ans après un fils qui, du destin sévère
Reçut de jours hélas, deux fois moins que son père.

15. Bien entendu, elle ne date pas de Diophante. Elle serait due à Metrodore (vers 500 ?).

De quatre ans, dans les pleurs, celui-ci survécut.
Dis, si tu sais compter, à quel âge il mourut.

Si d est l'âge auquel Diophante est mort, la traduction des hypothèses donne $\frac{d}{6} + \frac{d}{12} + \frac{d}{7} + 5 + \frac{d}{2} + 4 = d$ c'est-à-dire $d = 84$.

1.4 Les constructions à la règle et au compas

Dès l'Antiquité, la règle et le compas sont les outils essentiels des architectes et des artistes. C'est un domaine où les Grecs excellent et, pour l'essentiel, ils savent réaliser toutes les constructions actuellement connues, mais on verra qu'ils échouent sur d'autres. Dans tout ce qui suit, construire signifie : à la règle et au compas.

La question fondamentale est ici la suivante :

(QC)	Quelles sont les constructions possibles et comment les réaliser ?

1.4.1 Le pentagone régulier

Par exemple, et c'est l'un des sommets de la mathématique grecque, Euclide sait construire un pentagone régulier à la règle et au compas, en construisant pour cela un triangle d'angles $72°, 72°, 36°$ (Livre IV prop. 10 et 11). Voilà comment on peut procéder, avec une méthode proche de celle d'Euclide, mais en utilisant toutefois certains outils plus récents.

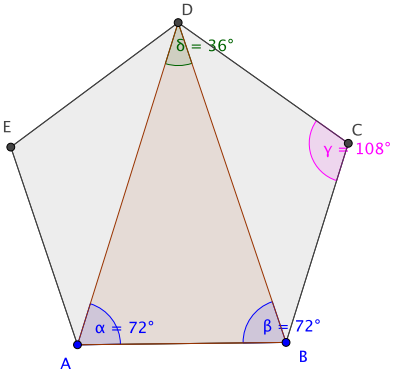

FIGURE 2 –

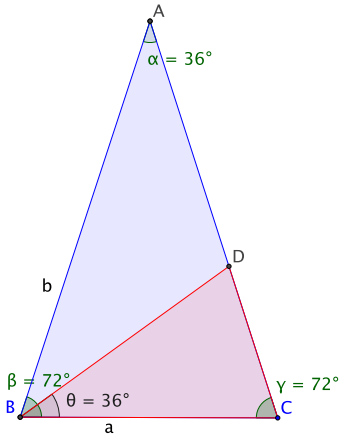

FIGURE 3 –

Rappelons qu'un pentagone régulier a tous ses côtés égaux et tous ses angles égaux. On note d'abord, en décomposant le pentagone en trois triangles, que la somme de ses angles est de 540°, donc que chacun de ses angles vaut 108°. Puis, en considérant les triangles isocèles latéraux, on voit que leurs angles à la base valent 36° et on en déduit que les angles du triangle central valent 72°, 72° et 36°, voir figure 2. Si l'on sait construire ce triangle on saura donc construire le pentagone.

Pour cela, si ABC est le triangle à construire, on trace la bissectrice de l'angle $\widehat{B}$, qui coupe $[AC]$ en D, voir figure 3. Les triangles ABC et BCD sont semblables (car ils ont des angles de 72°, 72° et 36°). On pose $a = BC$ et $b = AB = AC$. Comme BCD et ABD sont isocèles, on a $BC = BD = AD = a$ donc $CD = b - a$ et la proportionnalité des côtés donne $\dfrac{b-a}{a} = \dfrac{a}{b}$ ou encore $b^2 - ab - a^2 = 0$. Si l'on pose $\varphi = b/a$, ce nombre vérifie l'équation $\varphi^2 - \varphi - 1 = 0$ et il vaut donc $\varphi = \dfrac{1+\sqrt{5}}{2}$ (c'est le fameux nombre d'or).

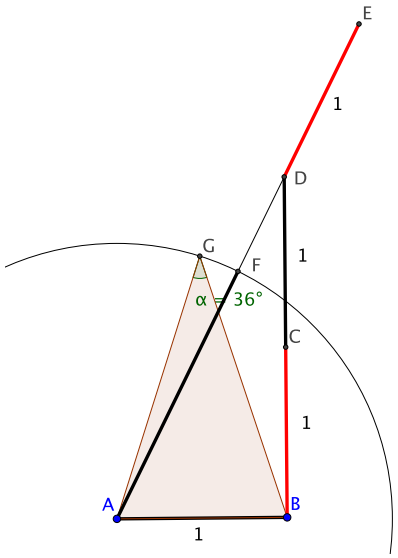

FIGURE 4 – Construction du nombre d'or

Il reste à construire φ à partir de l'unité. C'est facile, on construit un triangle rectangle de côtés 1 et 2, son hypoténuse vaut $\sqrt{5}$, on la prolonge d'une unité et on prend le milieu, voir figure 4.

1.4 *Remarque.* Attention, si le passage par le triangle $36-72-72$ est bien la méthode utilisée par Euclide, en revanche, il n'utilise pas du tout les calculs

tels que nous avons les menés ci-dessus avec le nombre d'or. D'une manière générale, les Grecs n'utilisent pas beaucoup les nombres, même les rationnels, qui ne sont vus que comme des rapports de longueurs. C'est la grande faiblesse de la mathématique grecque qui sera surmontée par Descartes.

1.4.2 Les échecs des Grecs

Malgré leur expertise, les Grecs échouent sur quatre problèmes de constructions à la règle et au compas que nous expliquons ci-dessous.

Un cube d'arête a étant donné, peut-on construire un cube de volume double (donc d'arête $b = a\sqrt[3]{2}$) ?

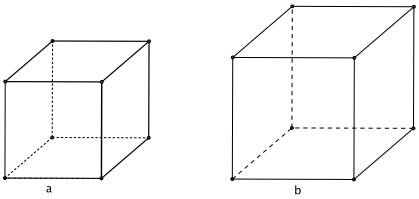

FIGURE 5 – La duplication du cube

Peut-on construire l'angle égal au tiers de 60° ?

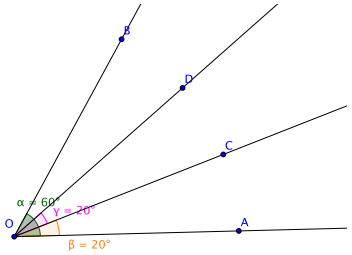

FIGURE 6 – La trisection de l'angle

Peut-on construire un carré d'aire égale à celle d'un disque donné ?

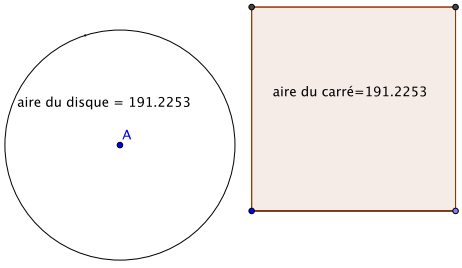

FIGURE 7 – La quadrature du cercle

On a vu qu'Euclide sait construire le pentagone régulier (et bien sûr aussi triangle équilatéral, carré, hexagone, octogone), mais peut-on construire l'heptagone régulier ou les polygones réguliers à 9 ou 17 côtés ?

Cet exemple mérite discussion. En effet, il faut bien comprendre que toutes ces constructions sont possibles **de manière approchée** (car on sait construire tous les nombres rationnels), mais il s'agit de savoir si une construction **exacte** existe. Voici un exemple avec l'heptagone. Pour le construire, on part de l'hexagone régulier et du triangle équilatéral obtenu en prenant un sommet sur deux de l'hexagone. Si a est la moitié du côté de ce triangle et si l'on reporte a sur le cercle, on trace un heptagone qui semble régulier à l'œil, mais ne l'est pas tout à fait, voir figure ci-dessous.

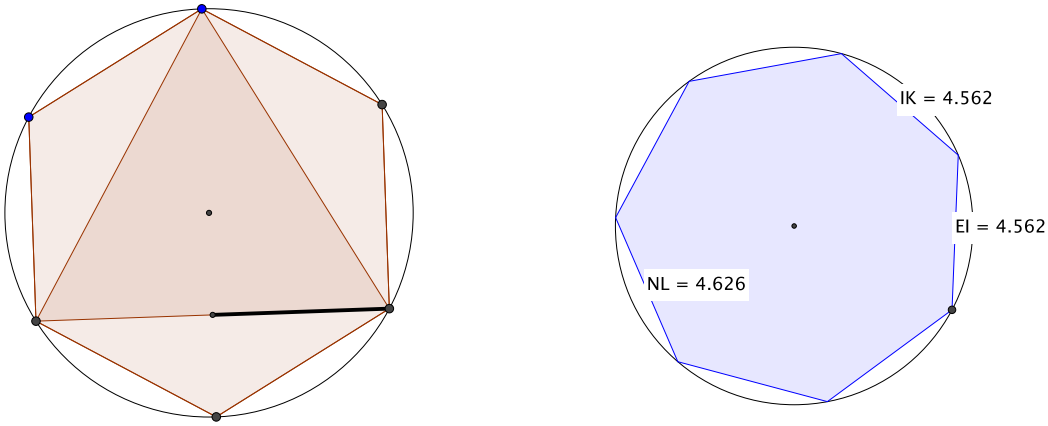

FIGURE 8 – Une construction approchée de l'heptagone

2 La période intermédiaire : de la Renaissance à 1900

2.1 Les nombres premiers

2.1.1 Fermat et Mersenne

On a vu qu'il y a une infinité de nombres premiers, mais la question [16] se pose d'en trouver d'arbitrairement grands. Pierre de Fermat (vers 1600-1665) pensait avoir trouvé une formule donnant à coup sûr des nombres premiers. Voilà ce qu'il dit :

16. Qui reste tout à fait actuelle.

Mais voici ce que j'admire le plus : c'est que je suis quasi persuadé que tous les nombres progressifs augmentés de l'unité, desquels les exposants sont des nombres de la progression double, sont nombres premiers, comme 3, 5, 17, 257, 65537, 4 294 967 297 et le suivant de 20 lettres 18 446 744 073 709 551 617; etc. Je n'en ai pas la démonstration exacte, mais j'ai exclu si grande quantité de diviseurs par démonstrations infaillibles, et j'ai de si grandes lumières, qui établissent ma pensée, que j'aurois peine à me dédire.

En langage mathématique actuel, il s'agit des nombres $F_n = 2^{2^n} + 1$ pour $n \geq 0$. Les cinq du début $(3, 5, 17, 257, 65537)$ sont bien premiers. Vérifions le (de tête) pour 257.

Il suffit de voir qu'il n'a pas de diviseur premier. Or, il n'est évidemment pas multiple de 2, ni de 5. Pour 3 on a le critère bien connu de la somme des chiffres : $2 + 5 + 7 = 14$ n'étant pas multiple de 3, 257 ne l'est pas non plus. Pour 7, une petite ruse : si 257 était multiple de 7, $250 = 257 - 7$ le serait aussi, mais $250 = 25 \times 10 := 5 \times 5 \times 5 \times 2$ n'est pas multiple de 7. Pour 11 on a un critère analogue à celui de 3 : un nombre écrit en système décimal $n = \overline{abc}$ est multiple de 11 si et seulement si $a - b + c$ l'est. (Il suffit de noter que $n = 100a+10b+c = 99a+a+11b-b+c = 11(9a+b)+a-b+c$.) Or ici on a $2 - 5 + 7 = 4$. Il n'est pas non plus multiple de 13, sinon $257 + 13 = 270 = 3^3 \times 2 \times 5$ le serait. Le nombre premier suivant est 17. Mais il est inutile de considérer ce cas car si l'on avait $257 = 17 \times a$, comme $17 \times 17 = 289 > 257$, a serait < 17 et aurait un facteur premier déjà examiné. On voit que 257 est bien premier.

Pour $65537 = 2^{16} + 1$ on pourrait utiliser la même procédure, mais cela prendrait un peu de temps et les machines font ça bien mieux que nous. En utilisant par exemple le logiciel SAGE on voit que 65537 est bien premier. En revanche, SAGE affirme que $2^{32} + 1$ ne l'est pas et même que 641 le divise ! Fermat se serait donc trompé ?

C'est vrai et on peut comprendre pourquoi $p = 641$ divise $2^{32} + 1$. Pour cela, on calcule "modulo p", autrement dit en regardant seulement les restes [17] dans la division par p. On s'intéresse aux puissances de 2. Dans 641 on voit 64 et même 128 car $641 = 5 \times 128 + 1 = 5 \times 2^7 + 1$. Modulo p on a donc $5 \times 2^7 \equiv -1$. Pour approcher 2^{32} on élève à la puissance 4 : $5^4 \times 2^{28} \equiv 1 \pmod{p}$. Mais, 5^4 c'est 625 et on a $641 = 625 + 16$, autrement dit, modulo 641, on a $5^4 \equiv -2^4$ et donc $-2^4 \times 2^{28} \equiv 1$, soit $2^{32} \equiv -1$ et c'est ce qu'on voulait.

2.1 *Remarque.* On ignore aujourd'hui encore s'il y a d'autres nombres de Fermat qui sont premiers. Tous ceux qu'on connaît sont composés, mais on

17. Travailler modulo p, c'est faire un peu comme la Mafia : quand on voit p, on flingue !

n'a la réponse que pour un nombre fini d'entre eux. Le plus grand connu est $F_{2747497}$ qui est composé, le plus petit dont on ignore s'il est premier ou non est F_{33}.

Faute de Fermat, on utilise, pour trouver de grands nombres premiers, les nombres de Mersenne $M_n = 2^n - 1$. Bien entendu, tous ne sont pas premiers, par exemple $15 = 2^4 - 1$. On montre facilement (exercice) qu'il faut que n soit premier, mais ce n'est pas suffisant (ainsi $2^{11} - 1 = 2047 = 23 \times 89$). Il n'empêche que c'est avec ces nombres qu'on obtient les records du plus grand nombre premier [18]. On peut citer ainsi le nombre $M_{19} = 524287$ trouvé par Cataldi en 1588, puis M_{127} de 39 chiffres trouvé par Lucas en 1876 (Lucas a inventé un critère très efficace pour voir si un nombre de Mersenne est premier, critère encore utilisé de nos jours [19]). On a ensuite, parmi d'autres, $M_{6972593}$ (plus de 2 millions de chiffres, 1999). *Exercice : montrer que ce nombre commence par* 437075 *et finit par* 193791. Enfin, le record actuel est $M_{82589933}$ trouvé le 7 décembre 2018. Il a 24 millions de chiffres, soit près de 10000 pages d'un livre qui ne contiendrait que les chiffres de ce nombre.

2.1.2 Dirichlet

À partir de la deuxième dizaine, les nombres premiers ne peuvent se terminer que par $1, 3, 7, 9$ et l'expérience montre qu'on en trouve régulièrement avec ces quatre finales. La question est de savoir s'il y en a effectivement une infinité. C'est un cas particulier d'un théorème de Dirichlet (1838) :

2.2 Théorème. *Il existe une infinité de nombres premiers dont l'écriture décimale se termine par* $1, 3, 7$ *ou* 9.

On peut même préciser qu'il y en a "autant" de chaque type. La preuve est difficile, voir [5]. Je me contenterai de montrer un point très facile :

Il existe une infinité de nombres premiers se terminant par 3 *ou* 7.

Sinon on en a un nombre fini $p_1 = 3$, $p_2 = 7$, $p_3 = 13$, etc. jusqu'à p_n et on regarde $N := 10p_2p_3 \cdots p_n + 3$ (qui se termine par 3) et ses diviseurs premiers $q_1, \ldots, q_r$. Ils sont distincts de 3 et des autres p_i, donc ils sont $> p_n$. Ils ne peuvent se terminer tous par 1 ou 9 car un produit de nombres se terminant par 1 ou 9 se termine par 1 ou 9 (on a $1 \times 1 = 1$, $1 \times 9 = 9$, $9 \times 9 = 81$). Donc il y en a qui se terminent par 3 ou 7 et c'est une contradiction.

18. Disons le plus grand nombre premier **connu** car on a vu qu'il y en a une infinité, donc pas de plus grand.

19. Voir, sur ma page web :
`https://www.imo.universite-paris-saclay.fr/~daniel.perrin/CAPES/arithmetique/Lucas.pdf`

On peut aussi montrer, de manière relativement élémentaire, l'infinitude de ceux qui se terminent par 1 (voir [1]) et on en fabrique en regardant les diviseurs des entiers de la forme $n^4 - n^3 + n^2 - n + 1$ pour $n \geq 2$, ou encore de ceux qui se terminent par 9, et on en fabrique en regardant les diviseurs des entiers de la forme $5n^2 - 1$. En revanche, pour être sûr de l'infinitude de ceux qui se terminant par 3 **et** par 7, c'est plus difficile.

2.1.3 Des questions ouvertes

Toujours sur cette question des finales des nombres premiers, on peut se demander s'il y a beaucoup de dizaines "riches" comme celle des 10, où les quatre nombres possibles sont premiers : $11, 13, 17, 19$. On voit tout de suite qu'il n'y en a pas d'autre jusqu'à 100, mais que $101, 103, 107, 109$ sont premiers, ainsi que les nombres de la dizaine des 190 ou des 820. Une expérience utilisant le logiciel SAGE montre ainsi qu'il y a 165 dizaines riches jusqu'à 1000000 et on peut conjecturer :

2.3 Conjecture. *Il y a une infinité de dizaines riches.*

Cette conjecture implique évidemment la suivante :

2.4 Conjecture. (Les nombres premiers jumeaux) *Il y a une infinité de nombres premiers jumeaux, c'est-à-dire qui diffèrent de* 2.

Ces deux conjectures sont très plausibles, et pourtant, on ne sait toujours pas les démontrer (voir ci-dessous).

Pour voir qu'il n'est pas facile de prédire si une question ouverte est facile ou non, le lecteur pourra montrer, à titre d'exercice, l'existence d'une infinité de dizaines pauvres (sans nombres premiers), la première étant celle des 200, voire de centaines pauvres, voire l'existence d'un milliard (ou de tout autre entier n) de nombres de suite sans nombres premiers [20].

Toujours sur les nombres premiers, citons aussi :

2.5 Conjecture. (L'hypothèse de Goldbach, 1742) *Tout nombre pair* ≥ 4 *est somme de deux nombres premiers.*

L'expérience confirme : $4 = 2+2$, $6 = 3+3$, $8 = 5+3$, $10 = 5+5 = 7+3$, $12 = 7+5$, $14 = 7+7 = 11+3$, $16 = 13+3$, $18 = 11+7$, $20 = 13+7$, etc.

20. La recette est d'utiliser $n! = 1 \times 2 \times 3 \times \cdots \times n$.

2.1.4 Le théorème des nombres premiers

Le résultat le plus important du XIX^e siècle sur les nombres premiers est dû, indépendamment, à Hadamard et De la Vallée-Poussin et il date de 1896 :

2.6 Théorème. *Soit x un réel positif. On note $\pi(x)$ le nombre de nombres premiers $\leq x$. Alors on a $\pi(x) \sim \dfrac{x}{\ln x}$ quand x tend vers l'infini.*

Cela signifie que le rapport de ces deux quantités tend vers 1 lorsque x devient grand. Ce théorème est essentiel, mais le résultat reste assez imprécis car l'erreur est très importante encore. Ainsi, on a $\pi(10^8) = 5\,761\,455$ et $10^8/\ln(10^8) \simeq 5\,428\,681$. La démonstration est très difficile et repose sur une fonction étudiée notamment par Bernhardt Riemann (1826-1866), la fonction ζ (zeta) définie (pour $\Re(s) > 1$) par $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. D'ailleurs l'approximation de $\pi(x)$ serait grandement améliorée si le résultat suivant était prouvé :

2.7 Conjecture. (Hypothèse de Riemann, 1859) *La fonction $\zeta(s)$ de la variable complexe s n'a pas de zéros non triviaux en dehors de la droite $\Re(s) = \frac{1}{2}$ (partie réelle de s égale $1/2$).*

2.2 Les équations algébriques

À la fin du Moyen-âge, l'équation du second degré est bien maîtrisée (dans le cas de racines réelles, évidemment) et la question se pose de résoudre des équations de degré plus grand (que les mathématiciens arabes notamment ont rencontrées). C'est en Italie que le progrès essentiel va être accompli.

2.2.1 Cardan et les autres

On cherche les racines de l'équation[21] $x^3 + px + q = 0$. L'astuce de Cardan[22] consiste à poser $x = u + v$ en introduisant deux inconnues au lieu d'une. L'intérêt – non évident *a priori* – est d'avoir un degré de liberté supplémentaire. L'équation devient alors :

$$u^3 + v^3 + (u + v)(3uv + p) + q = 0.$$

C'est ici que se révèle l'intérêt de l'astuce. Comme on a deux inconnues u, v, on peut leur imposer une relation supplémentaire, et ici, on va imposer

21. On montre facilement qu'on peut se ramener à ce cas.

22. Il n'est pas évident que ce soit Cardan qui ait le premier trouvé cette méthode. D'autres noms circulent : Scipion del Ferro (1515), Tartaglia (1535) et les controverses sur la primeur ont été sanglantes. Mais Cardan a eu le mérite de publier un traité *Ars Magna* qui rassemble tous les résultats connus à l'époque (1545).

$3uv+p=0$ (relation $(*)$), ce qui tue un des termes et il reste $u^3+v^3+q=0$. On constate alors qu'on connaît la somme $u^3+v^3=-q$ et le produit $u^3v^3=-\dfrac{p^3}{27}$ grâce à $(*)$. Quand on a la somme S et le produit P de deux nombres, on sait qu'ils sont racines de l'équation du second degré $Y^2-SY+P=0$. Ici, u^3 et v^3 sont donc racines de $Y^2+qY-\dfrac{p^3}{27}$ (équation $(**)$).

On connaît donc u^3 et v^3, on extrait leurs racines cubiques u et v et on trouve x comme $u+v$, obtenant ainsi une résolution "par radicaux" :

$$x=\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{4p^3+27q^2}{4\times 27}}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{4p^3+27q^2}{4\times 27}}}.$$

Cette formule relativise l'intérêt de la méthode : les calculs auxquels elle conduit peuvent être parfois compliqués. De plus, pour avoir des valeurs approchées des solutions, il faut calculer des racines carrées ou cubiques, ce qui n'est pas forcément simple.

2.2.2 La quête des degrés ≥ 5

Dans la foulée de Cardan, un de ses élèves[23], Ferrari, traite le cas de l'équation du quatrième degré en 1540. Dès lors, on cherche, sans succès, une méthode analogue pour les équations de degré ≥ 5. Les travaux de Vandermonde et Lagrange en 1770 mènent à l'idée que ce n'est pas possible. Voilà ce que dit Lagrange :

Il résulte de ces réflexions qu'il est très douteux que les méthodes dont nous venons de parler puissent donner la résolution complète des équations du cinquième degré et à plus forte raison celle des degrés supérieurs.

La preuve de cette impossibilité est donnée en 1824 par le mathématicien norvégien Niels Abel (1802-1829) pour le degré 5 puis en 1832 par Évariste Galois (1811-1832) pour tous les degrés, grâce à l'invention de la théorie qui porte son nom et qui repose essentiellement sur une notion nouvelle et fondamentale : celle de groupe.

Ces résultats closent la recherche sur ce point de la résolution exacte par radicaux, mais, heureusement, on peut trouver des solutions approchées, aussi importantes dans la pratique. Il y a de nombreuses méthodes pour cela, la plus efficace ayant été inventée par Newton en 1669, mais cela nous ferait sortir de nos thèmes pour rentrer dans le domaine de l'analyse.

23. Un autre point très important est l'invention par Bombelli, en 1572, des nombres imaginaires pour traiter le cas où l'équation de degré 3 a trois racines réelles, voir [3].

FIGURE 9 – Niels Abel

FIGURE 10 – Évariste Galois

2.3 Les équations diophantiennes

2.3.1 Bachet et Fermat

On appelle ici équation de Bachet l'équation en nombres entiers $x^3 = y^2 + d$ où d est un entier donné.

L'équation $x^3 = y^2 + 2$ a été étudiée pour la première fois en 1621 par Gaspard Bachet de Méziriac qui, à partir de la solution évidente $x = 3, y = 5$ $(27 = 25 + 2)$, a donné une méthode pour construire d'autres solutions **rationnelles**.

FIGURE 11 – Gaspard Bachet de Méziriac

La méthode est la suivante. Si l'on a une solution rationnelle (a, b) de $x^3 = y^2 + d$, on cherche une solution $x = a + h$, $y = b + k$ en imposant que la droite qui joint ces deux points soit tangente à la courbe. On obtient ainsi

$x = \dfrac{9a^4 - 8ab^2}{4b^2} \quad y = \dfrac{8b^4 + 27a^6 - 36a^3b^2}{8b^3}$. Avec $d = 2$ on a $\frac{129}{100}$, $\frac{383}{1000}$.

Pierre de Fermat, lui, cherche des solutions **entières** :

Peut-on trouver en nombres entiers un carré autre que 25 qui, augmenté de 2, fasse un cube ? À la première vue cela paraît d'une recherche difficile ; en fractions une infinité de nombres se déduisent de la méthode de Bachet ; mais la doctrine des nombres entiers, qui est assurément très belle et très subtile, n'a été cultivée ni par Bachet, ni par aucun autre dans les écrits venus jusqu'à moi.

FIGURE 12 – Pierre de Fermat

Dans le cas $d = 4$, voilà ce qu'il écrit à son correspondant anglais Digby en 1657 :

Je lui avais écrit (à Frénicle) *qu'il n'y a qu'un nombre carré entier qui, joint au binaire, fasse un cube, et que ledit carré est 25, auquel, si vous ajoutez 2, il se fait 27, qui est un cube. Il a peine à croire cette proposition négative, et la trouve trop hardie et trop générale. Mais, pour augmenter son étonnement, je dis que, si l'on cherche un carré qui, ajouté à 4 fasse un cube, il ne s'en trouvera jamais que deux en nombres entiers, savoir 4 et 121, car 4 ajouté à 4 fait 8 qui est un cube et 121 ajouté à 4 fait 125 qui est aussi un cube ; mais, après cela, toute l'infinité des nombres n'en saurait fournir un troisième qui ait la propriété.*

On ignore comment Fermat pouvait procéder pour prouver ces résultats. C'est d'ailleurs habituel chez lui, comme en témoigne l'exemple de son "grand théorème". En effet, dans la marge de son édition des œuvres de Diophante, Fermat écrit :

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duas ejusdem nominis fas est dividere : cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Traduction : *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 de même degré : j'en ai découvert*

une démonstration véritablement merveilleuse que cette marge est trop étroite pour contenir.

En termes mathématiques : pour $n \geq 3$, l'équation $x^n + y^n = z^n$ n'a pas de solution avec $x, y, z \neq 0$. On ne sait pas si Fermat avait vraiment une preuve de ce théorème [24]. Toujours est-il que le grand théorème de Fermat a suscité beaucoup de recherches des mathématiciens depuis le XVII^e siècle.

2.3.2 Kümmer

En 1847 Kümmer a accompli l'un des progrès les plus significatifs sur le grand théorème de Fermat en utilisant les nombres complexes.

Je vais tenter d'expliquer le point de départ de la méthode de Kümmer sur le cas (plus simple) de l'équation de Bachet $x^3 = y^2 + d$.

On a vu avec l'équation de Pythagore $x^2 + y^2 = z^2$ tout l'intérêt qu'il pouvait y avoir à factoriser les expressions. Malheureusement, ici, $y^2 + d$, avec $d > 0$, ne se factorise pas, en tous cas pas dans les entiers, car $-d$ n'est pas un carré. On va pourtant le factoriser en utilisant les nombres complexes (appelés aussi "imaginaires") et notamment le nombre [25] $i = \sqrt{-1}$. Avec ce nombre on écrit $x^3 = y^2 + d = (y + i\sqrt{d})(y - i\sqrt{d}) := z\overline{z}$ et, pour avoir un cube dans le premier membre, il suffit que les deux morceaux du second membre soient des cubes. On essaie donc de trouver un nombre de la même forme $w := a + ib\sqrt{d}$ tel que $(a + ib\sqrt{d})^3 = y + i\sqrt{d}$. En calculant le cube par la formule $(u + v)^3 = u^3 + 3u^2v + 3uv^2 + v^3$ on obtient :

$$y + i\sqrt{d} = a^3 + 3a^2bi\sqrt{d} - 3ab^2d - ib^3d\sqrt{d}.$$

Si l'on sépare les parties réelles et imaginaires, cela nous mène à deux équations : $y = a^3 - 3ab^2d$ et $1 = 3a^2b - b^3d$, qui sont des équations dans $\mathbf{Z}$.

On regarde la deuxième équation. On est dans les entiers et on voit que b doit diviser 1. Ah, mais 1, c'est encore pire qu'un nombre premier, il n'a pas de diviseurs autres que lui-même et son opposé. On a donc $b = \pm 1$, d'où $d = 3a^2 \pm 1$ (ce qui nous donne donc une condition nécessaire sur d pour avoir des solutions par cette méthode) et on obtient $y = a^3 - 3ad$ et $x = a^2 + d$ (car $x^3 = z\overline{z}$ est le cube de $w\overline{w} = a^2 + d$). Vite, on vérifie ! Si l'on en croit ce calcul, on doit avoir, si $d = 3a^2 \pm 1$:

$$(a^2 + d)^3 = (a^3 - 3ad)^2 + d,$$

24. Aucun mathématicien sérieux ne pense cela.

25. Dans ce qui suit, le lecteur est invité à calculer sans crainte avec ces nombres, même s'il n'en maîtrise pas tous les secrets.

et on constate, avec ravissement, que c'est vrai [26] ! On obtient ainsi, par exemple, avec $a = 2$, pour $d = 3a^2 + 1 = 13$, la solution $x = 17$, $y = 70$ et pour $d = 3a^2 - 1 = 11$, $x = 15$ et $y = 58$.

2.4 Les constructions

2.4.1 Descartes

Il y a beaucoup de tentatives vaines au Moyen-âge (notamment des mathématiciens arabes) pour résoudre les quatre problèmes des Grecs. L'opinion la plus courante, à partir du XVII^e siècle, est qu'ils sont impossibles. Voilà ce que dit Kepler :

L'heptagone, à la différence du pentagone ne peut pas se construire à la règle et au compas. Le compas et la règle sont les seuls outils permis en géométrie classique. Or la géométrie est le seul langage qui nous rende capable de comprendre les ressorts de l'esprit divin. Donc les figures que l'on ne peut construire à la règle et au compas − comme les polygones à 7,11,13 ou 17 côtés − sont en quelque sorte impures car elles sont un défi à l'intelligence. Elles sont non existantes.

Le grand progrès, qui va permettre de résoudre les problèmes des Grecs est dû à Descartes, c'est l'invention de la géométrie analytique et de l'usage des coordonnées [27]. Voilà ce qu'il dit :

Tous les problèmes de géométrie se peuvent facilement réduire à tels termes, qu'il n'est besoin par après que de connoître la longueur de quelques lignes droites pour les construire.

Et comme toute l'arithmétique n'est composée que de quatre ou cinq opérations, qui sont l'addition, la soustraction, la multiplication, la division et l'extraction des racines, qu'on peut prendre pour une espèce de division, ainsi n'a-t-on autre chose à faire en géométrie touchant les lignes qu'on cherche pour les préparer à être connues, que de leur en ajouter d'autres, ou en ôter ; ou bien en ayant une, que je nommerai l'unité pour la rapporter d'autant mieux aux nombres, et qui peut ordinairement être prise à discrétion, puis en ayant encore deux autres, en trouver une quatrième qui soit à l'une de ces deux comme l'autre est à l'unité, ce qui est le même que la multiplication ; ou bien en trouver une quatrième qui soit à l'une des deux comme l'unité est à l'autre, ce qui est le même que la division ; ou enfin trouver une ou deux, ou plusieurs moyennes proportionnelles entre l'unité et quelque autre ligne, ce qui est le même que tirer la racine carrée ou cubique, etc. Et je ne craindrai

26. Même si cette méthode n'est pas entièrement justifiée, elle a fourni cependant un résultat pas du tout évident.

27. Et cela réalise la jonction des thèmes 2 et 4.

pas d'introduire ces termes d'arithmétique en la géométrie, afin de me rendre plus intelligible.

2.4.2 La solution

C'est seulement au XIX^e siècle que la situation se dénoue, et d'abord en un sens positif car Gauss montre que le polygone régulier à 17 côtés est constructible.

Cependant la plupart des résultats obtenus sont négatifs : la duplication du cube et la trisection de l'angle (Pierre-Laurent Wantzel, 1837, à l'aide des équations algébriques et de la théorie de Galois), la quadrature du cercle (Lindemann, 1882) sont impossibles.

Pour les polygones réguliers, disons à un nombre premier [28] p de côtés, on montre que les seuls constructibles sont ceux pour lesquels p est un nombre ... de Fermat : $3, 5, 17$, 257, 65537, (et peut-être d'autres ?).

2.4.3 Un aperçu de l'impossibilité de la duplication du cube

Pour comprendre ce résultat il faut penser résolument en termes de nombres. On part de l'arête du cube, que l'on peut voir dans le plan comme un segment de longueur 1 et on appelle 0 et 1 ses extrémités. À partir de ces deux nombres on construit facilement les nombres entiers, positifs ou négatifs, à la règle et au compas, puis les rationnels (en utilisant Thalès) et aussi les racines carrées (on a vu ci-dessus $\sqrt{5}$, pour le reste on consultera [2]). En fait, on ne peut guère construire autre chose. En effet, toute construction revient à prendre l'intersection de deux droites ou cercles. Quand on prend deux droites $y = ax + b$ et $y = \alpha x + \beta$ on obtient des nombres qui se calculent rationnellement à partir des coefficients. Dans le cas d'un cercle $x^2 + y^2 + ax + by + c = 0$ et d'une droite $y = \alpha x + \beta$, en remplaçant y par sa valeur dans l'équation du cercle on obtient une équation de degré 2 que l'on résout avec la racine carrée du discriminant. Il en est de même dans le cas de deux cercles (en commençant par retrancher les équations).

Pour formaliser ce qu'on obtient ainsi, il faut introduire la notion de **corps**. Il s'agit d'un ensemble de nombres dans lequel on peut faire les quatre opérations : addition, soustraction, mutiplication, division), comme les rationnels ou les réels. Si l'on part d'un corps K et qu'on ajoute à K la racine $\sqrt{d}$ d'un élément de K on obtient un nouveau corps, noté $K(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in K\}$ (on vérifie qu'il s'agit bien d'un corps).

28. Pour un n quelconque il faut que n soit de la forme $2^\alpha p_1 \cdots p_r$ où les p_i sont des nombres premiers de Fermat distincts.

Ce qu'on voit alors c'est que si un nombre est constructible, il est dans l'étage du haut d'une **tour** de corps :

$$\mathbf{Q} \subset K_1 = \mathbf{Q}(\sqrt{d_1}) \subset K_2 = K_1(\sqrt{d_2}) \subset \cdots \subset K_n = K_{n-1}(\sqrt{d_{n-1}})$$

obtenus en ajoutant à chaque pas des racines carrées.

Mais, pour la duplication du cube, le nombre qu'il faudrait construire est $\sqrt[3]{2}$. Or on a le lemme suivant (voir [2]) :

2.8 Lemme. *Si $\sqrt[3]{2}$ est dans $K(\sqrt{d})$ il est déjà dans K.*

Si l'on admet ce lemme, on voit que si $\sqrt[3]{2}$ est constructible il est dans un K_n en haut d'une tour, et en le descendant grâce au lemme, on voit qu'il est dans $\mathbf{Q}$. Mais c'est impossible car il serait de la forme p/q avec p, q entiers premiers entre eux et on aurait $p^3 = 2q^3$. Il en résulte que p est pair, $p = 2p'$. Mais alors on a $4p'^3 = q^3$ donc q est pair aussi et c'est absurde.

Il reste à prouver le lemme. Si $\sqrt[3]{2}$ est dans $K(\sqrt{d})$ il s'écrit $a + b\sqrt{d}$ avec $a, b \in K$ et on a $(a + b\sqrt{d})^3 = 2$, donc $a^3 + 3a^2b\sqrt{d} + 3ab^2d + b^3d\sqrt{d} = a^3 + 3ab^2d + \sqrt{d}(3a^2b + b^3d) = 2$. On peut supposer $\sqrt{d} \notin K$ sinon le résultat est évident. Mais cela n'est possible que si l'on a $a^3 + 3ab^2d = 2$ et $3a^2b + b^3d = 0 = b(3a^2 + db^2)$. Comme $3a^2 + db^2$ est positif on obtient $b = 0$, puis $a^3 = 2$, donc $a = \sqrt[3]{2}$ est dans K.

2.4.4 Nouvelles techniques, nouveaux problèmes

On a vu que nombre de problèmes, qui remontaient souvent à l'Antiquité, ont été résolus au XIX^e siècle. Le plus souvent c'est grâce à l'utilisation de méthodes et de notions nouvelles, par exemple la notion de groupe chez Galois ou celle de nombre complexe[29] chez Kümmer, ainsi qu celle d'idéal. Ces notions qui, à cette époque, ont un rôle d'outil, deviennent peu à peu des objets de recherche à part entière, avec de nouvelles questions et de nouveaux résultats et elles envahissent progressivement toutes les mathématiques (et la physique). Ainsi, l'hypothèse de Riemann ne peut se comprendre que si l'on étend la fonction ζ aux complexes.

3 L'époque actuelle : 1900-2022

3.1 Les problèmes de Hilbert

Au deuxième congrès des mathématiciens en 1900, David Hilbert(1862-1943) propose à ses collègues 23 problèmes ouverts dont la solution lui paraît

29. Inventée par Bombelli pour traiter le cas des équations de degré 3 qui admettent trois racines réelles.

importante. Parmi ces problèmes, certains sont aujourd'hui résolus (16, au moins partiellement), d'autres non (5), d'autres sont considérés comme mal posés (2).

FIGURE 13 – David Hilbert

Par rapport à nos thèmes, le problème 8 porte largement sur les nombres premiers (l'hypothèse de Riemann, le problème de Goldbach et celui des nombres premiers jumeaux). Le problème 10 porte sur l'existence d'un algorithme pour calculer les solutions des équations diophantiennes.

3.2 Le vingtième siècle

Le vingtième siècle voit un grand nombre de problèmes résolus. On peut citer, dans des domaines proches de ceux que nous avons abordés :

• Le théorème de Mordell-Weil (1922-1928) qui porte sur les équations diophantiennes associées aux courbes elliptiques.

• Le théorème de Faltings, dans le même domaine, mais sur des courbes plus générales. (1983).

• La classification [30] des groupes simples finis dans les années 1980.

• L'infinitude des nombres de Carmichaël (des nombres qui ressemblent aux nombres premiers, mais n'en sont pas, 1994).

• La preuve du grand théorème de Fermat par Andrew Wiles en 1995.

• Le théorème de Green-Tao sur les nombres premiers dans les progressions (2004).

30. On estime que ce résultat requiert environ 10000 pages de démonstration.

3.3 Les sept problèmes du millenium

Il s'agit de problèmes, chacun d'eux doté d'un prix d'un million de dollars offert par l'institut Clay, proposés au début des années 2000.

- L'hypothèse de Riemann (arithmétique et analyse complexe)
- La conjecture de Birch-Swinnerton-Dyer (arithmétique)
- La conjecture de Hodge (géométrie algébrique)
- Les équations de Navier-Stokes (analyse)
- Le problème $P = NP$ (algorithmique)
- La conjecture de Poincaré (topologie ; résolue par Perelman)
- La théorie de Yang-Mills (physique mathématique)

Nous avons déjà rencontré l'hypothèse de Riemann. Un autre problème qui relève de l'un de nos thèmes est la conjecture de Birch-Swinnerton-Dyer (BSD) qui concerne les courbes elliptiques, comme celle de l'équation de Bachet. En voici un aperçu.

On peut munir ce type de courbe d'une addition pour laquelle elle est un groupe abélien, voir figure ci-dessous. Le théorème de Mordell-Weil assure que ce groupe est produit d'un groupe de la forme $\mathbf{Z}^r$ par un groupe fini. Ce dernier est assez bien connu et la conjecture BSD donne la valeur de l'entier r à l'aide d'une fonction de la variable complexe (fonction L, analogue à la fonction ζ).

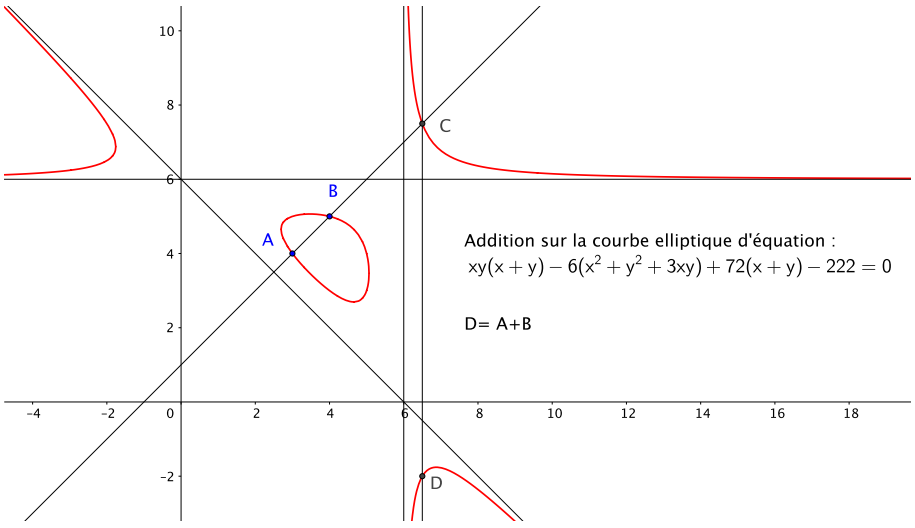

FIGURE 14 –

Pour les autres problèmes, il est à peu près impossible d'expliquer à des

lycéens de quoi il s'agit [31]

3.4 Le point sur deux autres conjectures

3.4.1 Goldbach

La conjecture de Goldbach est toujours ouverte. Voici quelques progrès récents sur ce thème.

• Vinogradov (1937) Tout nombre impair assez grand est somme de trois nombres premiers.

• Chen Jigrun (1966) Tout nombre pair assez grand et somme d'un premier et d'un nombre admettant au plus deux facteurs premiers.

• Ramaré (1995) Tout nombre pair est somme de six nombres premiers au plus.

• Helfgott (2013) Tout nombre impair > 5 est somme de trois nombres premiers.

3.4.2 Les jumeaux

Il s'agit de montrer qu'il existe une infinité de nombres premiers jumeaux $(p, p+2)$. La conjecture est toujours vive. Voici quelques points notables.

• Le record de la plus grande paire de jumeaux trouvée : deux nombres de 388342 chiffres.

• Le meilleur résultat théorique actuel : il existe une infinité de paires de nombres premiers dont la différence est ≤ 246 (Gowers et Tao, 2014).

3.5 Bilan des quatre thèmes

Sur les nombres premiers, malgré beaucoup de progrès, il reste de nombreuses questions ouvertes (l'hypothèse de Riemann, les nombres premiers jumeaux, la conjecture de Goldbach, etc.)

Sur les équations diophantiennes, il y a aussi beaucoup de problèmes (la conjecture de Birch et Swinnerton-Dyer, l'équation de Bachet et bien d'autres).

Les deux autres problèmes peuvent être considérés comme résolus, mais *via* la théorie des groupes ils ont donné naissance à de nombreuses autres questions (le problème inverse de Galois, la théorie de Jacquet-Langlands, etc.)

31. En ce qui me concerne, je comprends l'énoncé de la conjecture de Poincaré (mais pas la démonstration qu'en a donné Perelman), un peu celle de Hodge, vaguement $P = NP$ et pas du tout Navier-Stokes et Yang-Mills.

3.6 D'autres sources de problèmes pour les mathématiciens

Nous avons vu que nombre de questions que se posent les mathématiciens ont leurs racines dans l'histoire, mais il y a bien d'autres provenances possibles.

• La physique est une grande pourvoyeuse de problèmes pour les mathématiques, la mécanique conduit aux équations différentielles, la thermodynamique aux équations aux dérivées partielles, les ondes aux séries de Fourier, la mécanique quantique aux espaces de Hilbert, la météorologie aux systèmes dynamiques, etc.

• C'est vrai aussi pour la chimie, la biologie (notamment l'épidémiologie !), l'informatique etc.

D'une manière générale, les mathématiques fournissent un cadre à toutes les disciplines qui travaillent avec des grandeurs et/ou des formes.

3.7 Et les applications ?

C'est un point important, même si ce n'est pas mon sujet aujourd'hui. Les mathématiques sont utiles dans de nombreux domaines, qu'il s'agisse de comprendre certains phénomènes ou de produire des applications pratiques. C'est assez clair pour des domaines comme l'analyse ou les statistiques. C'est moins évident notamment pour l'arithmétique et l'on pouvait penser par exemple, jusqu'à il y a peu de temps, qu'on n'étudiait les nombres premiers que *pour l'honneur de l'esprit humain* comme disait Jacobi. Avec les nouvelles techniques de cryptographie (par exemple le code RSA), ils ont pris une importance capitale dans de nombreux domaines. Il faut donc se garder de croire qu'il y a des mathématiques qui ne peuvent pas avoir d'applications.

3.8 Quelques pistes de réflexion

Dans cette promenade à travers les siècles et les mathématiques, on a vu affleurer de nombreuses questions souvent de nature philosophique.

Un exemple est la question de la preuve en mathématiques, par rapport à l'expérience et notamment la preuve de certaines impossibilités. Le grand public a beaucoup de peine à concevoir qu'on puisse prouver qu'une construction à la règle et au compas est impossible [32].

La question de la dualité entre mathématiques pures et appliquées, avec en particulier la discussion entre solution exacte et solution approchée est un

32. Et il y a des mathématiciens amateurs qui essaient encore aujourd'hui de trouver la trisection de l'angle bien qu'il soit démontré qu'elle est impossible.

autre point important. Dans la plupart des cas pratiques, dans les applications à la physique, les solutions approchées suffisent. Attention cependant aux systèmes dynamiques instables, popularisés sous le nom d'effet papillon, voir [4].

Enfin, la question des progrès en mathématiques est essentielle, avec l'explosion des nouvelles techniques et la profusion de nouveaux concepts, qui sont utilisés d'abord comme des outils avant de devenir des objets d'étude à part entière.

Je vous laisse méditer sur tout cela.

Références

[1] Perrin D., *Cours d'algèbre*, Ellipses, 1996.

[2] Perrin D. *Mathématiques d'école*, Cassini, 2011.

[3] Perrin D, *La méthode de Cardan et les imaginaires*
`https://www.imo.universite-paris-saclay.fr/~daniel.perrin/CAPES/algebre/Cardan10.pdf`

[4] Perrin D. *La suite logistique*
`https://www.imo.universite-paris-saclay.fr/~daniel.perrin/Conferences/logistiqueDP2.pdf`

[5] Serre J.-P. *Cours d'arithmétique*, PUF, 1970.

email : *daniel.perrin@universite-paris-saclay.fr*