« Beaucoup passeront et la science s'augmentera »

Jean Aymes(*)

Introduction

Fermat n'a pas publié d'ouvrage élaboré ; son « œuvre » considérable est connue par sa correspondance, des notes dans les marges, des textes épars. C'est un foisonnement d'inventions, l'amorce même de domaines nouveaux des Mathématiques (calcul infinitésimal ou probabilités). Il réussit à s'imposer, de son vivant, comme l'un des grands mathématiciens de son temps. Il a su convaincre, avec un style plus occupé à développer l'efficacité de méthodes qu'à l'exposition de preuves, résolvant et relançant le questionnement (par quelque défi) avec des exemples éprouvant la méthode. Permanente, tout de même, est la conscience de jouer justement un rôle. Ses écrits sont sensibles à la beauté, beauté des Mathématiques soulignée de nombreuses fois, une forme d'émerveillement. Manque de temps, de place, défaut de travail ou même de génie, souvent il fait des remarques à ce propos vis-à-vis de lui-même. Cela ne fait qu'augmenter la grandeur de ce rôle.

Communément le mot « arithmétique » renvoie au calcul pratique sur les nombres. Ce mot a eu jusqu'au XVI^{e} siècle un sens inspiré des Anciens Grecs, l'étude des relations abstraites reliant les nombres entiers.

Il semble que l'on doive à Adrien-Marie Legendre (1752-1833) la première appellation « Théorie des nombres » pour désigner l'étude des propriétés des nombres entiers. C'est de cette manière qu'il intitule son ouvrage sur la question paru pour la première fois en 1798 « *Essai sur la théorie des nombres* ». Un siècle et demi après les travaux de Fermat, dans la préface de son ouvrage, se livrant à un résumé de l'histoire de l'Arithmétique depuis les Anciens, faisant le constat, empli de regrets, de ce que l'œuvre de Fermat a d'incomplet, Legendre souligne ce que l'on doit à son illustre prédécesseur : « *Fermat, l'un des géomètres dont les travaux contribuèrent le plus à accélérer la découverte des nouveaux calculs, cultiva avec un grand succès la science des nombres et s'y fraya des routes nouvelles. On a de lui un grand nombre de théorèmes intéressants, mais il les a laissés presque tous sans démonstration. C'était l'esprit du temps de se proposer des problèmes les uns aux autres. On cachait le plus souvent sa méthode, afin de réserver des triomphes nouveaux tant pour soi que pour sa nation ; car il y avait surtout rivalité entre les géomètres français et les anglais. De là il est arrivé que la plupart des démonstrations de Fermat ont été perdues, et le peu qui nous en reste nous fait regretter d'autant plus celles qui nous manquent* ».

(*) jaymes.apmep@wanadoo.fr

La lettre à Carcavi

Ces « routes nouvelles », plusieurs textes nous les donnent à voir. Les deux grands défis de Fermat aux mathématiciens de 1657 écrits en latin, sa lettre à Digby[1] de juin 1658, sa lettre à Carcavi[2] de 1659 apparaissent comme bilans d'une œuvre, de par sa conscience de transmettre un flambeau, comme une forme de testament scientifique.
La lettre à Carcavi, à titre d'exemple, permet d'évoquer l'essentiel des « routes nouvelles », ouvertes par Fermat sur la mise en œuvre, particulièrement, de la descente infinie, routes plus tard empruntées et entretenues, prolongées, élargies par nombre des mathématiciens qui lui ont succédé.
Carcavi communiqua cette lettre à Huyghens[3] ; le texte connu est une copie à la main de celui-ci. Le texte ci-dessous est pris, à partir de la page 431, dans « Œuvres de Fermat », volume 2, publiées par les soins de Paul TANNERY et Charles HENRY, Gauthier-Villars, 1894.
(consultable à l'adresse : http://gallica.bnf.fr/ark:/12148/bpt6k6213616t/f455)
Au gré de cette lecture essayons de dessiner cet héritage : quelques commentaires sont proposés à côté du texte, ou lorsque la place manque, suivent l'extrait du texte.

Les paragraphes 1 et 2 :

C1 – Août 1659 C1 FERMAT A CARCAVI. Août 1639 (Corresp. Huyg, n° 631) RELATION DES NOUVELLES DECOUVERTES EN LA SCIENCE DES NOMBRES	
1. Et pour ce que les méthodes ordinaires, qui sont dans les Livres, étoient insuffisantes à démontrer des propositions si difficiles, je trouvai enfin une route tout à fait singulière pour y parvenir. J'appelai cette manière de démontrer la *descente infinie* ou *indéfinie*, etc. ; je ne m'en servis au commencement que pour démontrer les propositions négatives, comme, par exemple :	1. La lettre commence par deux problèmes dont l'impossibilité de triangle rectangle à côtés de longueurs entières et d'aire égale à un carré ; problème souvent évoqué dans les écrits de Fermat.
Qu'il n'y a aucun nombre, moindre de l'unité qu'un multiple de 3, qui soit composé d'un quarré et du triple d'un autre quarré ; *Qu'il n'y a aucun triangle rectangle en nombres dont l'aire soit un nombre quarré.*	*« La preuve se fait par réduction à l'absurde en cette manière. »* Fermat décrit le principe de la méthode : la descente

(1) Kenelm DIGBY (1603- 1665)
(2) Pierre de CARCAVI (vers 1603 – 1684)
(3) Christian HUYGENS (1629 – 1695)

La preuve se fait par « conduite vers l'impossible »(απαγωγήν είς άδύνατον) en cette manière :
S'il y avoit aucun triangle rectangle en nombres entiers qui eût son aire égale à un quarré, il y auroit un autre triangle moindre que celui-là qui auroit la même propriété. S'il y en avoit un second, moindre que le premier, qui eût la même propriété, il y en auroit, par un pareil raisonnement, un troisième, moindre que le second, qui auroit la même propriété, et enfin un quatrième, un cinquième, etc. à l'infini en descendant. Or est-il qu'étant donné un nombre, il n'y en a point infinis en descendant moindres que celui-là (j'entends parler toujours des nombres entiers). D'où on conclut qu'il est donc impossible qu'il y ait aucun triangle dont l'aire soit quarrée.
On infère de là qu'il n'y en a non plus en fractions dont l'aire soit quarrée ; car, s'il y en avoit en fractions, il y en aurait en nombres entiers, ce qui ne peut pas être, comme il se peut prouver par la *descente*.
Je n'ajoute pas la raison d'où j'infère que, s'il y avoit un triangle rectangle de cette nature, il y en auroit un autre de même nature moindre que le premier, parce que le discours en seroit trop long et que c'est là tout le mystère de ma méthode. Je serai bien aise que les Pascal et Roberval et tant d'autres savans la cherchent sur mon indication.

infinie qu'il vient d'élaborer à propos de questions d'entiers.

La démonstration est donnée dans l'observation 45 sur Diophante(4).
Cette propriété implique l'inexistence d'entier non nul bicarré qui soit somme de deux bicarrés ! Fermat a démontré son grand théorème pour l'exposant 4.

Et puis, pour terminer sur ce problème, exemplairement, une mise au défi … bien dans l'esprit du temps !

2. Je fus longtemps sans pouvoir appliquer ma méthode aux questions affirmatives, parce que le tour et le biais pour y parvenir est beaucoup plus malaisé que celui dont je me sers aux négatives. De sorte que, lorsqu'il me fallut démontrer que *tout nombre premier, qui surpasse de l'unité un multiple de 4, est composé de deux quarrés*[1], je me trouvai en belle peine. Mais enfin une méditation diverses fois réitérée me donna les lumières qui me manquoient, et les questions affirmatives passèrent par ma méthode, à l'aide de quelques nouveaux principes qu'il y fallut joindre par nécessité. Ce progrès de mon raisonnement en ces questions affirmatives est tel : si un nombre premier pris à discretion, qui surpasse de l'unité un multiple de 4, n'est point composé de deux quarrés, il y aura un nombre premier de même nature, moindre que le

2. À propos de la décomposition en deux carrés d'un nombre de la forme $4n+1$, une invocation de la descente infinie pour la preuve de ce beau résultat, positif cette fois : Fermat veut étendre le type de problèmes auxquels il entend appliquer la descente, et ne pas le restreindre à des impossibilités. Pour Fermat, c'est cette méthode de la descente qui rapproche ces problèmes, fait leur unité,

(4) DIOPHANTE d'Alexandrie 3e siècle après J.-C.

donné, et ensuite un troisième encore moindre, etc. en descendant à l'infini jusques à ce que vous arriviez au nombre 5, qui est le moindre de tous ceux de cette nature, lequel il s'ensuivroit n'être pas composé de deux quarrés, ce qu'il est pourtant. D'où on doit inférer, par la déduction à l'impossible, que tous ceux de cette nature sont par conséquent composés de deux quarrés.	produit une sorte de programme scientifique.

L'observation VII sur Diophante :

Dans ce paragraphe 2, la note 1 de la lettre, à la fin de l'énoncé de son théorème, renvoie à l'observation VII sur Diophante : Bachet de Méziriac[5] a publié en 1621 une traduction du grec au latin des ouvrages arithmétiques conservés de Diophante. Fermat a abondamment annoté ce livre en latin. (On trouve le texte latin à l'adresse : https://fr.wikisource.org/wiki/Œuvres_de_Fermat_-_I_-_Partie_2 - VI). Ses observations ne sont pas toujours brèves, comme en témoigne celle-ci avec un détail sur :
a) les nombres premiers de la forme $(4n + 1)$ hypoténuses de triangles rectangles [équation $(4n + 1)^2 = x^2 + y^2$], leurs puissances, leurs produits, puis les mêmes sommes de deux carrés [équation : $4n + 1 = x^2 + y^2$] ;
b) le nombre de façons différentes dont un nombre donné peut être hypoténuse de triangle rectangle ;
c) l'obtention d'un nombre entier qui soit hypoténuse de triangle rectangle d'autant de façons que l'on voudra ;
d) l'obtention d'un nombre qui soit somme de deux carrés d'autant de façons que l'on voudra.
e) le nombre de façons différentes dont un nombre donné est somme de deux carrés.

a) Traduit en français, Fermat écrit : « *Tout nombre premier, de la forme* $4n + 1$*, est une seule fois l'hypoténuse d'un triangle rectangle ; son carré l'est deux fois, son cube trois, son bicarré quatre, et ainsi de suite indéfiniment. Le même nombre premier et son carré sont, d'une seule façon, somme de deux carrés ; son cube et son bicarré le sont de deux façons ; sa cinquième et sa sixième puissance de trois façons, et ainsi de suite indéfiniment. Si un nombre premier, qui soit somme de deux carrés, est multiplié par un autre nombre premier, qui soit également la somme de deux carrés, leur produit sera, de deux façons différentes, somme de deux carrés ; si le multiplicateur est le carré du second nombre premier, le produit sera somme de deux carrés de trois façons différentes ; si le multiplicateur est le cube du second nombre premier, le produit sera somme de deux carrés de quatre façons différentes, et ainsi de suite indéfiniment.*»

b) Fermat énonce le nombre de décompositions en « hypoténuse de triangles rectangles », c'est-à-dire le nombre d'écritures de son carré comme somme de deux carrés d'entiers naturels, sans considération de l'ordre des termes. Il écrit : « *Il est*

(5) Claude-Gaspard BACHET dit de Méziriac (1581 – 1638)

facile (…) de déterminer de combien de façons différentes un nombre donné peut être hypoténuse d'un triangle rectangle ».
Comme souvent, Fermat procède en montrant sur un exemple.
Pour le nombre $N = 5^3 \times 13^2 \times 17$, il trouve 52 décompositions du carré N^2 comme somme de deux carrés ; son calcul se rapporte à une formule générale : pour $5^r \times 13^s \times 17^t$, le nombre de décompositions de son carré est

$$\frac{1}{2}\left[(2r+1)(2s+1)(2t+1)-1\right],$$

formule qu'on peut étendre à un nombre quelconque de facteurs premiers de la forme $(4n + 1)$ avec des exposants respectifs entiers quelconques.

c) Le problème est ainsi posé dans la traduction de l'*Observation 7* : « *Trouver un nombre premier qui soit hypoténuse d'autant de façons que l'on voudra* ». (texte latin original : « *Invenire numerum qui quoties quis velit sit hypotenusa*. »)
Fermat résout ici complètement une question que Bachet a simplement soulevée : trouver un nombre dont le carré soit décomposable en deux carrés de tant de manières que l'on voudra. Le traducteur du texte latin des *Observations* a commis un lapsus : c'est bien un nombre entier, non nécessairement premier que l'on cherche, pour qu'il soit représentable comme hypoténuse d'un triangle rectangle d'un nombre de façons donné. Fermat choisit 7 et exploite alors la formule

$$\frac{1}{2}\left[\text{produit de termes de la forme}(2r+1)-1\right]=7,$$

d'où

$$\left[\text{produit de termes de la forme}(2r+1)\right]=15\ ;$$

le produit valant 15, il a deux facteurs premiers 3 et 5, qui fournissent les exposants 1 et 2, et donc le produit de deux nombres premiers de la forme $4n + 1$ affectés de leurs exposants respectifs ainsi calculés donne le résultat.

d) Il s'agit de « *Trouver un nombre qui soit somme de deux carrés d'autant de façons que l'on voudra* » (texte latin original : « *Invenire numerum qui quoties quis velit componatur ex duobus quadratis*. »)
La question est ici reprise pour le nombre lui-même et non pour son carré. Pour 10 façons, il détermine un produit P de termes de la forme $(r + 1)$ tels que $\frac{1}{2}E(P) = 10$; il vient $P = 20$ se décomposant en $2 \times 2 \times 5$, pour donner les exposants 1, 1 et 4. Les nombres admettant exactement 10 décompositions sont de la forme abc^4 (a, b, c étant entiers, premiers de la forme $4n + 1$).

e) « *de combien de façons différentes un nombre donné est somme de deux carrés* »
C'est une mise en œuvre d'une formule non démontrée, sur deux exemples.
325 c'est $5^2 \times 13$; ses diviseurs premiers 5 et 13, de la forme $4n + 1$, avec pour exposants 2, 1. Fermat détermine un produit P de termes de la forme $(r + 1)$ correspondant, soit 6. Dont la moitié donne 3, nombre de manières d'écrire 325 comme somme de deux carrés ; en effet $325 = 15^2 + 10^2 = 13^2 + 14^2 = 17^2 + 6^2$.

Il examine ensuite, de la même façon, un nombre où la suite des exposants serait : 2 , 2, 1 ; la même formule lui donne : (2 + 1)(2 + 1)(1 + 1)/2 = 9
On savait depuis longtemps que le produit de sommes de carrés vérifie une paire d'égalités remarquables que l'on exprime sous la forme algébrique ainsi :

$$\left(a^2+b^2\right)\left(c^2+d^2\right)=\left(ac+bd\right)^2+\left(ad-bc\right)^2=\left(ac-bd\right)^2+\left(ad+bc\right)^2.$$

On peut penser que Diophante, d'une manière ou d'une autre (pas sous la forme algébrique citée, l'algèbre étant loin d'être en usage dans ces formes), connaissait ces égalités. C'est seulement au XIIIe siècle que l'on voit Fibonacci(6) les énoncer et les démontrer. Reprises par Bombelli(7), elles seront utilisées par Viète(8) pour engendrer de nouveaux triangles de Pythagore à partir de deux d'entre eux déjà connus. Fermat travaille cela, cette relation a pu lui servir à obtenir le nombre de toutes les décompositions d'un produit à partir de celles de chacun des facteurs.
Les questions de représentation d'un nombre comme sommes de carrés d'entiers sont apparues dès l'Antiquité, sans doute en liaison avec le théorème de Pythagore. Diophante savait qu'un nombre de la forme $4n + 3$ ne peut être la somme de deux carrés, qu'un nombre de la forme $8n + 7$ ne peut être somme de trois carrés. Tout nombre entier peut-il être écrit comme somme de quatre carrés ? Au XVIIe siècle, Bachet de Méziriac l'énonce comme conjecture, il a poussé la vérification jusqu'à 325. Fermat affirme l'avoir prouvé.
Depuis l'Antiquité, ces questions n'ont cessé de susciter une foule de nouveaux problèmes, dont l'étude constitue une des parties les plus étendues et les plus florissantes de la théorie des nombres. Le questionnement sur les sommes de carrés est véritablement un problème prolifique.
L'énoncé du théorème général de la décomposition d'un entier naturel en somme de deux carrés n'a été donné pour la première fois, semble-t-il, qu'en 1801, par Karl Friedrich Gauss(9), dans ses *Disquisitiones Arithmeticae* (Recherches arithmétiques) ; celles-ci, novatrices, proposent une synthèse unificatrice de l'étude des problèmes sur les nombres entiers et tirent parti de liens féconds avec les autres branches des Mathématiques.
Pour l'entier N, supérieur ou égal à deux, dont la décomposition en facteurs premiers est $2^m p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$ où les nombres premiers p_i sont de la forme $4n + 1$ et les entiers q_j sont de la forme $4n + 3$, en posant $A = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ et $B = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$:
– si B n'est pas un carré : il n'y a pas de décompositions en somme de deux carrés
– sinon, ce nombre de décompositions est le même pour les nombres N et A et vaut $4\left[\left(a_1+1\right)\left(a_2+1\right)\cdots\left(a_r+1\right)\right]$.
Ici : si $(x ; y)$ est solution, alors $(\pm x ; \pm y)$ et $(\pm y ; \pm x)$ sont solutions ; on a vu que Fermat ne comptait pas ainsi. En divisant par 8, on retrouve la formule utilisée ci-dessus par Fermat pour un produit de nombres premiers de la forme $(4n + 1)$.

(6) Leonardo FIBONACCI (vers 1175 - vers 1250)
(7) Raphaël BOMBELLI (1526-1572)
(8) François VIETE (1540 – 1603)
(9) Karl Friedrich GAUSS (1777 – 1855)

Les paragraphes 3 et 4 de la lettre à Carcavi

3. 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 quelquefois si malaisée qu'on n'y peut 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, jusques là qu'il confesse qu'il la juge si difficile qu'il ne voit point de voie pour la résoudre.(1) *Tout nombre est quarré ou composé de deux, de trois ou de quatre quarrés.* Je l'ai enfin rangée sous ma méthode et je démontre que, si un nombre donné n'étoit point de cette nature, il y en aurait un moindre qui ne le seroit 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.	On sait par les « Lettres de Monsieur Descartes(10) », que celui-ci écrivit à Mersenne(11) en juillet 1638 : « *…pour ce théorème, qui est sans doute l'un des plus beaux qu'on puisse trouver touchant les nombres, je n'en sais point la démonstration, et je la juge si difficile que je n'ose entreprendre de la chercher …* » Note (1) : le problème des quatre carrés, voir ci-dessous.
4. Celle que j'avais proposée à M. Frénicle et autres (2) est d'aussi grande ou même plus grande difficulté : *Tout nombre non quarré est de telle nature qu'il y a infinis quarrés qui, multipliant ledit nombre, font un quarré moins 1*. Je la démontre par la *descente* appliquée d'une manière toute particulière. J'avoue que M. Frénicle a donné diverses solutions particulières et M. Wallis aussi, mais la démonstration générale se trouvera par la *descente* dûment et proprement appliquée : ce que je leur indique, afin qu'ils ajoutent la démonstration et construction générale du théorème et du problème aux solutions singulières qu'ils ont données.	Note (2) : l'équation de Pell-Fermat, voir ci-dessous.

Le problème des quatre carrés

Ce problème s'est posé beaucoup plus tôt. Diophante fait l'hypothèse que tout nombre entier peut être écrit comme somme d'au plus quatre carrés d'entiers. Dans une lettre à Pascal(12) en 1654, Fermat énumère les étapes d'une démonstration qui n'a jamais été retrouvée. Vers 1750, lorsqu'il en a connaissance, Euler(13) est vivement impressionné et stimulé par les affirmations de Fermat, il parvient à

(10) René DESCARTES (1596 – 1650)
(11 Marin MERSENNE (1588 – 1648)
(12) Blaise PASCAL (1623 – 1662)
(13) Leonhard EULER (1707 – 1783)

montrer qu'il suffit de chercher les nombres premiers décomposables en somme de carrés, car le produit de deux nombres somme d'au plus quatre carrés est encore de cette forme. Lagrange[14] démontre ensuite en 1770 le théorème qui porte son nom : *tout nombre entier peut s'écrire comme somme de un, deux, trois ou quatre carrés de nombres entiers*.
(Par exemple $7 = 2^2 + 1^2 + 1^2 + 1^2$; $65 = 6^2 + 4^2 + 3^2 + 2^2 = 6^2 + 5^2 + 2^2 = 7^2 + 4^2 = 8^2 + 1^2$).
Euler apporte ensuite des simplifications à la preuve de Lagrange. On doit à Legendre, en 1785, un complément subtil pour les trois carrés : *tout nombre entier qui n'est pas de la forme* $4^r(8n + 7)$ *peut s'écrire comme somme de trois carrés au plus*, résultat qui s'inscrit dans des conjectures de Fermat.
Depuis plusieurs autres démonstrations ont été trouvées.
Plus généralement, le théorème des nombres polygonaux que Fermat donne dans sa lettre à Digby de juin 1658 sera établi par Cauchy en 1813. Ce sujet fait déjà partie d'une observation sur Diophante : voici ce qu'écrit Fermat, dans son observation XVIII, à propos de la proposition de Bachet : « Tout nombre est soit carré, soit somme de 2, 3 ou 4 carrés entiers. »

> « *Bien plus, il y a une proposition très belle et tout à fait générale que j'ai été le premier à découvrir :*
> *Tout nombre est : soit triangle, soit somme de 2 ou 3 triangles ;*
> *Soit carré, soit somme de 2, 3, 4 carrés ;*
> *Soit pentagone, soit somme de 2, 3, 4 ou 5 pentagones ;*
> *Et ainsi de suite indéfiniment qu'il s'agisse d'hexagones, d'heptagones ou de polygones quelconques ; cette merveilleuse propriété pouvant s'énoncer en général en raison du nombre des angles.*
> *Je ne puis ici donner la démonstration, qui dépend de nombreux et abstrus mystères de la Science des nombres ; j'ai l'intention de consacrer à ce sujet un Livre entier et de faire accomplir ainsi à cette partie de l'Arithmétique des progrès étonnants au delà des bornes anciennement connues.* »

Ce grand ouvrage ne verra pas le jour, la postérité devra ici aussi faire son œuvre.

Le problème de Waring[15], qui énonça sa conjecture pour des puissances supérieures à 2 en 1762, fut résolu par Hilbert en 1909 : « *Pour chaque entier naturel k, il existe un nombre s tel que tout entier positif soit somme de s puissances k-ièmes d'entiers positifs*. ». Cela n'épuise pas le sujet, par exemple s'il s'agit d'en savoir davantage sur les liens entre s et k. La détermination du plus petit s, noté $g(k)$ reste un problème ouvert. Le problème des 4 carrés dit que $g(2) = 4$.
Ce type de question, à point de départ dans l'Antiquité, est exemplaire de la prolixité d'un problème !

(14) Joseph-Louis LAGRANGE (1736 – 1813)
(15) Edward Waring, 1736-1798

L'équation de Pell[16]-Fermat

Autrement dit, Fermat affirme : « pour un nombre entier a non carré, il y a une infinité de nombres x et y tels que : $ay^2 = x^2 - 1$ » ; l'équation $x^2 - ay^2 = b$ est désignée comme « équation de Pell-Fermat ». Cette dénomination est impropre : l'apparition du nom de Pell est due à Euler qui se serait mépris sur le rôle de Pell à ce sujet. Reste que « équation de Fermat » convient mieux pour une autre formule assurément encore plus importante encore, celle du grand théorème.

Ce problème a une origine ancienne. Le problème des bœufs d'Hélios, attribué à Archimède, induit un cas particulier, complexe d'équation de Pell-Fermat ; on n'est parvenu à le traiter qu'à la fin du XIX^e siècle.

L'Hindou Brahmagupta[17] au VII^e siècle détaille des exemples de $x^2 - Ny^2 = 1$ avec N = 61 et N = 67 en donnant une règle pour obtenir une solution.

L'Hindou Bhaskara[18] au VII^e siècle énonce une règle de composition qui permet d'obtenir d'autres solutions. Avec la notation indicielle moderne, à partir d'une solution connue $(x_1 ; y_1)$, en posant : $x_{n+1} = x_1x_n + Ny_1y_n$ et $y_{n+1} = y_1x_n + x_1y_n$, si $(x_n ; y_n)$ est solution alors $(x_{n+1} ; y_{n+1})$ l'est aussi. De là une infinité de solutions s'il y en a une. Il développe le procédé d'obtention de solution des hindous ; pour $x^2 - 61y^2 = 1$, il fournit la solution (1766319049 ; 226153980) ; plus tard on prouvera que cette solution engendre toutes les autres.

Ces éléments ne semblent pas avoir été connus en Europe au XVII^e siècle.

Fermat propose le problème dans son « Second défi aux mathématiciens » en février 1657, selon la traduction du latin : « *Étant donné un nombre non carré quelconque, il y a une infinité de carrés déterminés tels qu'en ajoutant l'unité au produit de l'un d'eux par le nombre donné, on ait un carré.* » Il propose de traiter trois exemples : $3y^2 + 1 = x^2$, $149y^2 + 1 = x^2$, $109y^2 + 1 = x^2$.

Il s'en est suivi, durant quelques années, une importante correspondance entre l'Angleterre (Wallis[19], Brouncker[20]) et le continent (Fermat, Frénicle[21], Huygens) qui explique pour une part les propos de Legendre sur la « *rivalité entre les géomètres français et les anglais* ». Les Anglais proposent une méthode proche du procédé hindou ; elle répond aux exemples proposés par Fermat, mais ne règle pas le problème en général. Cette méthode utilise une succession de changements de variable, de la forme $x = my + z$, convenablement choisis ; pour en donner une idée sur un exemple élémentaire :

De l'équation $x^2 - 14y^2 = 1$, par $x = 3y + z$, on passe à l'équation $z^2 + 6yz - 5y^2 = 1$, puis par les changements de variable successifs $y = z + a$; $z = 2a + b$; $a = b + c$, on obtient : $b^2 - 6bc - 5c^2 = 1$.

Or cette équation admet une solution aisément visible : $c = 0$, $b = 1$; d'où une remontée des changements de variable pour atteindre une solution : $x = 15$ et $y = 4$.

(16) John PELL (1611 – 1685)
(17) BRAHMAGUPTA (598–668)
(18) BHASKARA II (1114 - 1185)
(19) John WALLIS (1616 – 1703)
(20) William BROUNCKER (1620 – 1684)
(21) Bernard FRENICLE de Bessy (première décennie du XVI^e siècle – 1674)

De tels changements de variables, déjà pratiqués par Bachet pour résoudre l'équation $ax + by = 1$ (Bachet-Bézout), sont liés au développement en fraction continue de $\sqrt{N}$.

Ici $\sqrt{14} = 3+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{6+\cdots}}}}}$, les quotients partiels donnant les coefficients m des changements de variable successifs. L'efficacité exemplaire du procédé n'élude pas les questions, au contraire : quel est son degré de généralité ? Cette solution particulière est-elle susceptible d'engendrer les autres ? Quelles sont les propriétés de ces fractions continues (ainsi nommées par Wallis) ? Qu'en est-il des formes quadratiques binaires ($Ax^2 + Bxy + Cy^2$, A, B, C entiers) ?

À propos de l'équation de Pell-Fermat, Fermat a évoqué un usage de la descente infinie, mais on ne connaît pas sa méthode : a-t-il voulu la cacher ?

Euler reprend le problème, retrouve les procédés des hindous et développe la connaissance des fractions continues et des formes quadratiques.

Lagrange publie en 1768 la première preuve complète faisant le lien entre toute solution de l'équation de Pell-Fermat et le développement en fraction continue de $\sqrt{N}$: existence d'une solution et moyen de la trouver, une infinité de solutions sont obtenues à partir de l'une d'elles, toutes les solutions de $x^2 - Ny^2 = 1$ s'obtiennent à partir du développement en fraction continue de $\sqrt{N}$.

Le questionnement s'élargit, l'accent est mis sur l'étude des formes quadratiques qui deviennent un centre d'intérêt de plus en plus important ; avec deux questions principales, pour une forme quadratique donnée, « quels entiers représente-t-elle ? », et « peut-on trouver toutes les représentations d'un entier donné ? ». L'étude des nombres de la forme $u + v$ (u, v entiers, puis u, v rationnels) commence à mettre l'accent sur ce qui sera bientôt rattaché aux structures algébriques (anneaux, corps).

C'est avec Gauss, dans ses *Disquisitiones Arithmeticae* (Recherches arithmétiques) que commence vraiment la théorie des formes quadratiques : il introduit notamment les notions d'équivalence de formes et de discriminant d'une forme.

On le voit, à nouveau, ce problème de l'équation de Pell-Fermat a véritablement joué un rôle considérable dans l'émergence de la théorie des nombres et de l'algèbre moderne.

Le 10e problème de Hilbert(22), posé en 1901, porte sur le sujet : « Trouver un *algorithme* déterminant si une équation diophantienne a des solutions ». En 1970, le mathématicien russe Matiassevitch(23) montrera que c'est impossible.

(22) David HILBERT (1862 – 1943)
(23) Iouri Vladimirovitch MATIASSEVITCH né en 1947

Paragraphe 5

5. J'ai ensuite considéré certaines questions qui, bien que négatives, ne restent pas de recevoir très grande difficulté, la méthode pour y pratiquer la descente étant tout à fait diverse des précédentes, comme il sera aisé d'éprouver. Telles sont les suivantes : *Il n'y a aucun cube divisible en deux cubes*.(3) *Il n'y a qu'un seul quarré en entiers qui, augmenté du binaire, fasse un cube. Le dit carré est 25.* *Il n'y a que deux quarrés en entiers, lesquels, augmentés de 4, fassent un cube. Les dits quarrés sont 4 et 121.* *Toutes les puissances quarrées de 2, augmentées de l'unité, sont nombres premiers.* Cette dernière question est d'une très subtile et très ingénieuse recherche et, bien qu'elle soit conçue affirmativement, elle est négative, puisque dire qu'un nombre est premier, c'est dire qu'il ne peut être divisé par aucun nombre. Je mets en cet endroit la question suivante dont j'ai envoyé la démonstration à M. Frénicle, après qu'il m'a avoué et qu'il a même, témoigné dans son Ecrit imprimé qu'il n'a pu la trouver : *Il n'y a que les deux nombres 1 et 7 qui, étant moindres de l'unité qu'un double quarré, fassent un carré de même nature, c'est-à-dire qui soit moindre de l'unité qu'un double quarré.*	Liste de 4 problèmes (3) Cette note (3) renvoie à la célébrissime observation II sur Diophante : « *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.* » Cinquième problème

Ce paragraphe débute par une liste de quatre affirmations qu'on peut réécrire aujourd'hui sous la forme :

– La reprise dans le cas de l'exposant 3, de l'observation II en marge du Diophante : c'est la « conjecture » appelée à devenir le grand théorème, démontré trois siècles et demi plus tard.

– L'équation $x^2 + 2 = y^3$ a une seule solution en nombres entiers (5 ; 3).

– L'équation $x^2 + 4 = y^3$ a exactement deux solutions en nombres entiers (2 ; 2) et (11 ; 5).

– Les nombres de la forme $2^{2^n}+1$ sont premiers ; ainsi 2, 5, 17, 257, 65 537.

Puis, Fermat affirme la solution d'un cinquième problème qui s'écrirait aujourd'hui : l'équation $2x^2-1=\left(2y^2-1\right)^2$ a pour seules solutions (1 ; 1), (7 ; 5).

La lettre à Digby

La lettre à Digby de juin 1658 contient une liste de problèmes encore plus abondante : à côté de quelques questions géométriques, on y trouve des questions non mentionnées dans la lettre à Carcavi, questions d'importance dans le paysage profilant la théorie des nombres. Ainsi :
– Tout nombre premier de la forme $3n + 1$ s'écrit sous la forme $x^2 + 3y^2$.
- Tout nombre premier de la forme $8n + 1$ ou $8n + 3$ s'écrit sous la forme $x^2 + 2y^2$.
- À propos des nombres polygonaux, à nouveau, sujet que Fermat juge très important : « *tout nombre entier est soit triangle, soit somme de deux ou trois triangles ; soit carré, soit somme de deux, trois ou quatre carrés ; soit pentagone, soit somme de deux, trois, quatre ou cinq pentagones ; soit hexagone, soit somme de deux, trois, quatre, cinq ou six hexagones ; et ainsi de suite en continuant indéfiniment*. ».
– Le double de tout nombre premier de la forme $8n - 1$ est somme de trois carrés.
- Le produit de deux nombres premiers se terminant par le chiffre 3 ou par le chiffre 7 s'écrit sous la forme $x^2 + 5y^2$.
- Un seul nombre triangulaire est bicarré, autrement dit : l'équation $x(x + 1) = 2y^4$ a une seule solution (1 ; 1).

Les nombres de Fermat

Les nombres de la forme $2^{2^n}+1$, appelés nombres de Fermat, sont devenus célèbres : ils sont l'objet d'une recherche qui se déploie alors. Mais Fermat se trompe en les annonçant premiers, ce qu'il affirme déjà par exemple dans une lettre à Frénicle dès 1640. Pourtant il ne modifiera jamais son affirmation, il l'écrit à Pascal le 29 août 1654, en fin de lettre à propos du problème des partis : « *C'est une propriété de la vérité de laquelle je vous réponds. La démonstration en est très malaisée et je vous avoue que je n'ai pas pu encore la trouver pleinement* ». Or le sixième nombre de la liste, $2^{32} + 1$, n'est pas premier, il est composé. C'est là une conjecture erronée de Fermat, chose rare.
Il revient à Euler, en 1732, d'apporter la réfutation. Celui-ci ne dévoile sa preuve que quinze ans plus tard.

Euler démontre que tout diviseur premier de $2^{2^n}+1$ est de la forme $2k \cdot 2^n + 1$. Ce qui « exclut grande quantité de diviseurs ». Essayant seulement les multiples successifs de 64 augmentés de 1 il trouve le diviseur 641 :

$$2^{32} + 1 = 641 \times 6\,700\,417.$$

C'est en 1780 seulement que Legendre montra que le septième nombre de la liste de Fermat, $2^{64} + 1$ est composé (divisible par 274 177).
Aujourd'hui, on ne connaît aucun nombre de Fermat premier autre que les cinq premiers de sa liste. On parvient, là aussi, à étudier des nombres de plus en plus grands. $2^{2^{33}}+1$ est le plus petit nombre de Fermat dont on ne sait pas aujourd'hui s'il est premier ou composé et en 2015, le plus grand nombre de Fermat dont on connaisse la factorisation complète est F_{11}. On conjecture que tous ces nombres sont

composés à partir d'un certain exposant, mais on ne sait pas montrer qu'une infinité d'entre eux sont composés.

Encore quelques questions, puis une conclusion aux accents lyriques

6. Après avoir couru toutes ces questions, la plupart de diverse nature et de différente façon de démontrer, j'ai passé à l'invention des règles générales pour résoudre les équations simples et doubles du Diophante. On propose par exemple, 2Q+7967 égaux à un quarré. J'ai une règle générale pour résoudre cette équation, si elle est possible, ou découvrir son impossibilité, et ainsi en tous cas et en tous nombres tant des quarrés que des unités.	Q désigne un carré
On propose cette équation double : 2N+3 et 2N+5 égaux chacun à un quarré. Bachet se glorifie, en ses Commentaires sur Diophante, d'avoir trouvé une règle en 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 rétabli la plupart des propositions défectueuses de Diophante et j'ai fait celles que Bachet avoue ne savoir pas et la plupart de celles auxquelles il paroit que Diophante même a hésité, dont je donnerai des preuves et des exemples à mon premier loisir.	Fermat est magistrat, il ne pratique les Mathématiques qu'à loisir ! Ce loisir qui lui fait trop défaut.
7. J'avoue que mon invention pour découvrir si un nombre donné est premier ou non n'est pas parfaite, mais j'ai beaucoup de voies et de méthodes pour réduire le nombre des divisions et pour les diminuer beaucoup en abrégeant le travail ordinaire. Si M. Frenicle baille ce qu'il a médité là-dessus, j'estime que ce sera un secours très considérable pour les savans.	
8. La question qui m'a occupé sans que j'aie encore pu trouver aucune solution est la suivante, qui est la dernière du Livre de Diophante *De multangulis numeris*.	
Dato numero, invenire quot modis multangulus esse possit.	« *Trouver de combien de manières un nombre donné peut être un (nombre) polygone*. »
Le texte de Diophante étant corrompu, nous ne pouvons pas deviner sa méthode ; celle de Bachet ne	

m'agrée pas et elle est trop difficile aux grands nombres. J'en ai bien trouvé une meilleure, mais elle ne me satisfait pas encore. 9. Il faut chercher en suite de cette proposition la solution du problème suivant : *Trouver un nombre qui soit polygone autant de fois plus qu'on voudra, et trouver le plus petit de ceux qui satisfont à la question*. 10. Voilà sommairement le compte de mes rêveries sur le sujet 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 savans pour trouver d'eux-mêmes ce que je n'étends point, principalement si MM. De Carcavi et Frénicle 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 connoître 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*.	

La conclusion de cette lettre est magnifique. Fermat y dit son sujet de prédilection : « *mes rêveries sur le sujet des nombres* ». Il entend « *transmettre le flambeau aux générations suivantes …* » et termine par : « *Beaucoup passeront et la science s'augmentera*. »

BIBLIOGRAPHIE

Œuvres de Pierre Fermat, La théorie des nombres, Roshdi RASHED, Christian HOUZEL, Gilles CHRISTOL, Albert Blanchard, 1999

Arithmétique pour amateurs, Marc GUINOT, sept livres, Aléas, 1992 à 2002

Abrégé d'histoire des Mathématiques, Jean DIEUDONNÉ et al., Hermann, 2007

*Mathématiques au fil des âge*s, I.R.E.M. Groupe Epistémologie et Histoire, Gauthier-Villars, 1987