LES CAS n=3, 4 et 5 DU THÉORÈME DE FERMAT.

Nous allons dans cet article donner quelques démonstrations «élémentaires» du théorème de Fermat dans des cas particuliers. Chacun sait qu'en mathématiques le mot «élémentaire» a un sens fort relatif ; il signifiera ici : compréhensible par un élève de Mathématiques Spéciales. Cependant, l'ingéniosité dont ont fait preuve Fermat, Euler et Dirichlet dans l'obtention de ces démonstrations dépasse largement ce niveau : seuls les outils sont élémentaires.
Soulignons tout d'abord deux points qui montrent la difficulté du problème, qui est masquée par la simplicité de son énoncé : l'équation $(E_n): x^n + y^n = z^n, x, y, z \in \mathbb{Z}^*$ n'a pas de solution pour $n > 2$. Cette conjecture devenue désormais théorème est maintenant célèbre, mais il faut bien réaliser qu'il n'y avait aucune raison a priori pour qu'il fût exact. Il n'est qu'à considérer des équations diophantiennes assez proches de (E_n) qui ont, elles, des solutions, à commencer par (E_2) : l'équation $x^3 + y^3 = z^3 + 1$ dont (9, 10, 12) est solution ou $x^3 + y^3 = z^2$ dont vous trouverez certainement une solution en chiffres, ou encore $x^3 + y^3 + z^3 = t^3$ dont le remarquable quadruplet (3, 4, 5, 6) est solution (si vous avez d'autres relations remarquables entre des puissances, envoyez-les nous !). Le deuxième point est d'ordre logique, et concerne tous les résultats «négatifs», où l'on démontre la non-existence d'une solution. L'on n'échappe pas dans ce cas à une démonstration par l'absurde où l'on va considérer une éventuelle solution (x, y, z) pour aboutir à une contradiction. Mais cette contradiction ne va intervenir qu'à la fin, et durant toute la démonstration, nous allons manipuler, additionner, diviser les nombres x, y et z, nombres dont nous savons pertinemment qu'ils n'existent pas, puisque justement, c'est ce que l'on est en train de prouver. Nous ne pourrons pas, comme on le fait d'habitude pour se rassurer, vérifier les calculs dans des cas particuliers, puisqu'il n'y a *pas* de cas particulier : il faut avoir beaucoup de foi pour travailler avec du vide!

La première réduction concernant ce théorème, très élémentaire, ce qui ne l'empêche pas d'être forte, est de le ramener aux valeurs premières de n. En effet, si (E_n) n'a pas de solution pour un certain n, la règle : $x^{kn} = (x^k)^n$ montre qu'elle n'en aura pour aucun multiple de n. Mais attention, (E_2) a des solutions ! Il va donc falloir démontrer que (E_4) n'en a pas et que (E_p) n'en a pas pour p premier impair. Et lorsque à la fin de cet article nous aurons démontré les cas n = 3, 4, 5, nous aurons réglé les cas de tous leurs multiples. Cependant le cas n = 14, bien que composé ne sera pas réglé ! Le cas n = 7 lui est indispensable.

I Le cas $n = 4$.

Nous commençons par lui, car c'est historiquement le premier cas démontré, et cela s'explique : c'est un cas à part puisque le seul à être non premier, et d'autre part les bicarrés (puissances quatrièmes) font partie du domaine des carrés, domaine qui est bien balisé, à commencer par la classique résolution de (E_2), que nous allons rappeler maintenant.

Théorème 1 : résolution de (E_2).

(x, y, z) est un triplet pythagoricien primitif (c'est-à-dire vérifiant $\boxed{x^2 + y^2 = z^2}$ avec x, y, z entiers naturels non nuls premiers entre eux) si et seulement s'il existe deux entiers naturels premiers entre eux et de parités distinctes $n > m > 0$ tels que :

$$\boxed{x = n^2 - m^2,\ y = 2nm,\ z = n^2 + m^2 \text{ ou } x = 2nm,\ y = n^2 - m^2,\ z = n^2 + m^2}.$$

Les triplets pythagoriciens quelconques s'obtiennent par produit d'un triplet primitif par un entier ≥ 1.

Démonstration du théorème 1 :
► Les entiers x, y, et z du triplet pythagoricien primitif sont plus que premiers entre eux globalement : ils le sont *2 à 2* (car si un nombre premier divisait deux d'entre eux, il diviserait le troisième). D'autre part, x et y ne peuvent être tous deux impairs car alors z serait pair donc z^2 divisible par 4, mais $x^2 + y^2 \equiv 2\ [4]$, car, modulo 4, un carré impair est congru à 1. Comme ils ne peuvent non plus être tous les deux pairs, *x et y sont de parités distinctes.* On peux donc supposer que x est pair et y impair (et donc z impair).
On peut alors écrire : $x = 2u,\ z + y = 2v,\ z - y = 2w$, avec $u, v, w \in \mathbb{N}^*$, et il est facile de voir que v et w sont aussi premiers entre eux. L'identité $x^2 = z^2 - y^2 = (z - y)(z + y)$ donne $u^2 = vw$, ce qui montre que v et w sont des carrés n^2 et m^2 (avec $n > m$ premiers entre eux) d'où $u = nm$ (exercice 1 : si le produit de deux entiers premiers entre eux est un carré, chacun d'eux est un carré et leurs racines carrées sont premières entre elles).
On a donc $x = 2u = 2nm,\ y = v - w = n^2 - m^2,\ z = v + w = n^2 + m^2$ et l'on vérifie que n et m n'ont pas la même parité puisque y et z sont impairs.
La réciproque est facile ; quant aux triplets pythagoriciens quelconques, il suffit de les diviser par le PGCD des trois nombres pour obtenir un triplet primitif. ◄

Nous avons donc obtenu une bijection entre les triplets pythagoriciens primitifs et les couples d'entiers > 0 premiers entre eux et de parités distinctes. Remarquons, et ce sera la clé de la résolution de (E_4) (de façon à abaisser le degré), que nous avons ainsi obtenu le fait que lorsqu'un carré est la somme de deux carrés premiers entre eux, il est impair et sa racine carrée est aussi la somme de deux carrés premiers entre eux. Remarquons également qu'un «triangle de Pythagore» (i.e. rectangle à côtés entiers non nuls) possède toujours une aire entière.

La résolution qui va suivre de l'équation de Fermat dans le cas $n = 4$, tirée de [Edwards], n'est pas due à Fermat proprement dit, ou du moins, on n'en a pas de trace. Mais elle est tout à fait comparable à d'autres démonstration qui nous restent de lui. Elle utilise en particulier le raisonnement par descente infinie qu'il a lui-même inventé et baptisé de ce nom : il ne peut y avoir de descente infinie dans l'ensemble des entiers naturels, ou, dans un langage moins poétique : dans un ensemble d'entiers naturels, il est impossible que pour tout élément, il y en ait un autre qui lui soit strictement inférieur, ce qui revient encore à dire qu'un ensemble non vide d'entiers naturels possède un plus petit élément.

Théorème 2

l'équation (E_4') : $\boxed{x^4 + y^4 = z^2}$ n'a pas de solution en entiers non nuls, ou, en français : **la somme de deux bicarrés non nuls ne peut être un carré**.

Ce résultat est plus fort que l'inexistence de solution pour (E_4), mais ce petit cadeau bonux ne demande aucun effort supplémentaire, c'est pourquoi nous ne nous en sommes pas privés.

Démonstration du théorème 2 :

► Supposons qu'il existe $x, y, z \in \mathbb{N}^*$ tels que $\boxed{x^4 + y^4 = z^2}$. Si un entier *d* divise *x* et *y*, d^4 divise z^2, donc d^2 divise *z* (exercice 2 : si un carré divise un carré, la racine carrée du premier divise la racine carrée du deuxième). Quitte à diviser *x* et *y* par leur PGCD et *z* par son carré, on peut donc supposer que *x* et *y* sont premiers entre eux ; le triplet (x^2, y^2, z) est donc pythagoricien primitif. On peut écrire, quitte à intervertir *x* et *y* :

$$x^2 = 2nm, \quad y^2 = n^2 - m^2, \quad z = n^2 + m^2.$$

La deuxième égalité signifie que (m, y, n) est encore un triplet de Pythagore, et il est primitif car *n* et *m* sont premiers entre eux. On sait que *n* est impair, et par conséquent, *m* est pair puisque *n* et *m* sont de parités contraires. On peut encore écrire :

$$m = 2pq, \quad y = p^2 - q^2, \quad n = p^2 + q^2,$$

avec *p* et *q* premiers entre eux, donc premiers avec *n*..

Cependant, comme $x^2 = 2nm = 4npq$, les entiers *n*, *p* et *q* sont tous les trois des carrés : $n = z'^2, p = x'^2, q = y'^2$ et la relation $\boxed{x'^4 + y'^4 = p^2 + q^2 = n = z'^2}$ montre que l'on a trouvé une nouvelle solution à l'équation de départ. Mais ceci est absurde par l'argument de descente infinie, car $0 < z' = \sqrt{n} \leq n^2 = z - m^2 < z$. ◄

Il est intéressant de donner maintenant une interprétation géométrique de ce résultat, que l'on pourrait désigner par «l'impossibilité de la quadrature du rectangle». Considérons une solution (*x*, *y*, *z*) de (E_4') (dont on sait maintenant qu'elle n'existe pas) : le rectangle de côtés x^2 et y^2 a une diagonale entière *z* et une aire carrée $(xy)^2$. Soit réciproquement un rectangle de côtés entiers > 0 *a* et *b* dont la diagonale est un entier *c*, et l'aire un carré. Quitte à diviser *a* et *b* par leur PGCD, on peut supposer que *a* et *b* sont premiers entre eux. Leur produit étant un carré, *a* et *b* sont des carrés x^2 et y^2, et l'on a $x^4 + y^4 = c^2$. On peut donc énoncer :

Corollaire 1 : **impossibilité de la quadrature du rectangle.**

Il n'existe pas de rectangle à côtés et diagonale entiers non nuls ayant la même aire qu'un carré à côtés entiers.

Ou encore : il n'existe pas de triangle de Pythagore dont l'aire soit le double d'un carré.

Ou enfin : on ne peut pas trouver deux carrés non nuls dont la somme et la racine carrée du produit soient tous deux des carrés.

Voici maintenant, traduit du latin par Tannery et Henri, et tiré de [Noguès], ce que l'on considère être la démonstration de Fermat de «son» théorème dans le cas *n* = 4 :

Si l'aire d'un triangle était un carré, il y aurait deux bicarrés dont la différence serait un carré ; il s'ensuit qu'on aurait également deux bicarrés dont la somme et la différence seraient des carrés. Par conséquent, on aurait un nombre carré, somme d'un carré et du double d'un carré, avec la condition que la somme des deux carrés qui servent à le composer soit également un carré. Mais, si un nombre carré est somme

d'un carré et du double d'un carré, sa racine est également somme d'un carré et du double d'un carré, ce que je puis prouver sans difficulté.
On conclura de là que cette racine est la somme de deux côtés d'un angle droit d'un triangle dont l'un des carrés composant formera la base et le double de l'autre carré la hauteur.
Ce triangle rectangle sera donc formé par deux nombres carrés dont la somme et la différence seront des carrés. Mais on prouvera que la somme de ces deux carrés est plus petite que ces deux carrés, dont on a également supposé que la somme et la différence soient des carrés. Donc, si ont trouve deux carrés dont la somme et la différence soient deux carrés, on donne par là même en nombre entiers deux carrés jouissant de la même propriété dont la somme est inférieure.
Part le même raisonnement, on aura ensuite une somme plus petite que celle déduite de la première et en continuant indéfiniment on trouvera toujours des nombre entiers plus petits satisfaisant aux mêmes conditions. Mais cela est impossible, puisque, un nombre entier étant donné, il ne peut y avoir une infinité de nombre entiers qui soient plus petits.

Ces raisonnements d'une densité exceptionnelle nécessitent pour nous, pauvres mortels, quelques éclaircissements. Tout d'abord, Fermat lie trois problèmes différents en apparence, dont nous allons montrer qu'ils sont en fait équivalents.

Problème 1 : **trouver deux bicarrés non nuls et distincts dont la différence est un carré (** $\boxed{x^4 - y^4 = z^2}$ **).**
Problème 2 : **trouver deux carrés non nuls dont la somme et la différence sont des carrés.**
Problème 2' : t**rouver trois carrés en progression arithmétique dont la raison est un carré non nul** (nous avons rajouté ce problème, car c'est une simple reformulation du problème 2).
Problème 3 (quadrature du triangle rectangle) : **trouver un triangle de Pythagore ayant la même aire qu'un carré à côtés entiers.**

Démonstration 1 : l'existence d'une solution au problème 1 implique l'existence d'une solution au problème 2.
► On a $x^4 - y^4 = z^2$, avec $x, y, z \in \mathbb{N}^*$. Comme dans le début de la démonstration du théorème 2, on peut se ramener au cas où x et y sont premiers entre eux. Soit alors d le PGCD de $x^2 + y^2$ et $x^2 - y^2$. Alors d divise $2x^2$ et $2y^2$ donc d= 1 ou 2. Si d = 1, comme $(x^2 + y^2)(x^2 - y^2) = x^4 - y^4 = z^2$, $x^2 + y^2$ et $x^2 - y^2$ sont des carrés, ce que nous voulions. Si d = 2, z= 2z' et $\frac{x^2 + y^2}{2} \times \frac{x^2 - y^2}{2} = z'^2$ donc $x^2 + y^2 = 2u^2$ et $x^2 - y^2 = 2v^2$. Mais alors $u^2 + v^2 = x^2$ et $u^2 - v^2 = y^2$.◄

Le passage du problème 2 au problème 2' est laissé au lecteur.

Démonstration 2 : l'existence d'une solution au problème 2' implique l'existence d'une solution au problème 3.

► Soient $a^2,\ b^2,\ c^2$ les trois carrés en progression arithmétique de raison $d^2 \neq 0$. Alors $(a+c)^2+(c-a)^2 = 2\left(a^2+c^2\right) = 4b^2$, et $\frac{1}{2}(a+c)(c-a) = \frac{c^2-a^2}{2} = d^2$. Le triangle de côtés $a+c,\ c-a,\ et\ 2b$ est donc un triangle de Pythagore d'aire carrée. ◄

Démonstration 3 : l'existence d'une solution au problème 3 implique l'existence d'une solution au problème 1.

► Soient a, b, c les côtés du triangle rectangle d'aire carrée ($a^2+b^2=c^2,\ ab=2d^2$) ; alors $c^4-(2d)^4 = \left(c^2-4d^2\right)\left(c^2+4d^2\right) = \left(a^2+b^2-2ab\right)\left(a^2+b^2+2ab\right) = \left(a^2-b^2\right)^2$. Nous avons bien trouvé deux bicarrés non nuls dont la différence est un carré. ◄

Ces trois problèmes étant donc équivalents, il suffit que l'un n'admette pas de solution pour qu'aucun n'en admette. Et chacun aura reconnu que le premier est un raffinement de (E_4), raffinement qui n'est d'ailleurs pas le même que celui du théorème 1 ($x^4+y^2=z^4$, au lieu de $x^4+y^4=z^2$). Il semble que l'intention de Fermat était de résoudre le problème 3, et que malgré les apparences, il fasse une descente infinie sur le problème 2. Quant à l'incursion du début dans le problème 1, elle semble ne devoir servir qu'à montrer que Fermat a bien démontré «son» théorème dans le cas n = 4. Si le lecteur désire une démonstration qui suive pas à pas celle de Fermat avec éclaircissement des points obscurs, il devra se reporter à [Edwards] page 10. Nous allons, nous, faire une descente infinie sur le problème 2, semblable à celle de la démonstration du théorème 2 ; d'ailleurs, je vais faire un «copier coller» sur le Mac.

Théorème 3

Les problèmes 1, 2, 3 ci-dessus n'ont pas de solution.

Avant de passer à la démonstration, pouvez-vous, en intermède, trouver trois carrés en progression arithmétique (de raison non carrée, bien sur) ? Pouvez-vous même les trouver tous ? (exercice 3 : la démonstration se trouve quasiment ci-dessus ; si vous séchez, reportez-vous à [Guinot 1] page 155).

► Supposons qu'il existe $x, y \in \mathbb{N}^*$ tels que $\boxed{x^2+y^2=a^2 \text{ et } x^2-y^2=b^2}$. Si vous supputez que l'on va se ramener au cas où *x* et *y* sont premiers entre eux, non seulement vous avez du flair, mais vous avez gagné! On a alors $y^4+z^2=x^4$ et le triplet $\left(y^2, z, x^2\right)$ est donc pythagoricien primitif. On peut écrire :

cas 1 : $y^2 = 2nm,\ z = n^2-m^2,\ x^2 = n^2+m^2$,

cas 2 : $z = 2nm,\ y^2 = n^2-m^2,\ x^2 = n^2+m^2$.

Le cas 2 est impossible car alors x^2-y^2 et x^2+y^2 seraient des doubles de carrés non nuls, or ce sont aussi des carrés par hypothèse (exercice 4 : un carré non nul ne peut être le double d'un carré).

La troisième égalité du cas 1 signifie que $(n,\ m,\ x)$ est encore un triplet de Pythagore, et il est primitif car *n* et *m* sont premiers entre eux. On peut encore écrire, quitte à intervertir *n* et *m* : $n = 2pq,\ m = p^2-q^2,\ x = p^2+q^2$, avec *p* et *q* premiers entre eux, donc premiers avec *m*.

Cependant, comme $y^2 = 2nm = 4mpq$, les entiers *m*, *p* et *q* sont tous les trois des carrés : $m = z'^2, p = x'^2, q = y'^2$. On a alors $\boxed{x'^4-y'^4 = p^2-q^2 = m = z'^2}$ et donc, comme dans la démonstration 1 on a deux cas :

Soit $x'^2 + y'^2$ et $x'^2 - y'^2$ sont des carrés, et dans ce cas, on a trouvé une nouvelle solution à l'équation de départ. Ceci est absurde par l'argument de descente infinie, car $0 < x' = \sqrt{p} < p^2 + q^2 = x$.
Soit $x'^2 + y'^2 = 2u^2$ et $x'^2 - y'^2 = 2v^2$ d'où $u^2 + v^2 = x'^2$ et $u^2 - v^2 = y'^2$ et ceci est aussi absurde car $0 < u \leq x' < x$ ◄

Lorsque l'on fait une démonstration qui ressemble à une autre, on peut se demander s'il n'y a pas redondance. En d'autres termes, ne pouvait-on pas montrer directement que les équations $\boxed{x^4 + y^4 = z^2}$ et $\boxed{x^4 - y^4 = z^2}$ sont équivalentes, puisque de toutes façon, d'un point de vue logique, elles le sont, n'ayant pas de solution ? Mais nous n'y sommes pas parvenus.
On peut en tout cas résumer ces deux résultats dans l'unique énoncé : il n'existe pas de triangle de Pythagore dont deux des côtés soient des carrés.

II Le cas *n* = 3.

Nous attaquons le plus petit nombre premier impair. D'une façon générale, puisqu'il y a plus d'entiers non divisibles par un nombre premier *p* donné que d'entiers divisibles par lui, on pourrait s'attendre à ce qu'il soit plus difficile de montrer que (E_p) n'a pas de solution en entiers premiers avec *p*, qu'en entiers dont l'un est multiple de *p*. C'est en fait le contraire qui se produit. Bien que cela ne serve pas dans la résolution générale de (E_3), nous allons commencer par la démonstration du fait que *x*, *y* ou *z* est divisible par 3, car c'est une simple mais jolie manipulation de congruences. Cette preuve ne sera pas directement généralisable à un nombre premier quelconque, mais on en verra plus loin une généralisation partielle sous la forme du théorème de Sophie Germain. C'est ce que l'on désigne par «premier cas de Fermat» : montrer que (E_p) n'a pas de solution avec les entiers *x, y* et *z* premiers avec *p*.

Lemme 1

si $\boxed{x^3 + y^3 = z^3}$, l'un des entiers *x*, *y* ou *z* est divisible par 3.

Démonstration du lemme 1.
► D'après le petit théorème de Fermat, ou tout simplement une vérification à la main, tout entier est congru à son cube modulo 3. Donc si $\boxed{x^3 + y^3 = z^3}$, $z \equiv x + y \ [3]$ et l'on peut écrire $z = x + y + 3k$. Si l'on travaille maintenant modulo 9, l'on peut écrire : $x^3 + y^3 = (x + y + 3k)^3 \equiv (x + y)^3 = x^3 + y^3 + 3xy(x + y)$ et par conséquent, $xy(x + y)$ est divisible par 3. Ceci montre que *x*, *y* ou *z* (qui est congru à *x* + *y* modulo 3) est divisible par 3. ◄

La démonstration générale se fait également par descente infinie. La version que nous allons en donner est due à Euler, mais le lecteur trouvera dans [Hardy & Wright] page 192 une démonstration située dès le départ dans $\mathbb{Z}[j]$.
De même que pour résoudre (E_4), nous avons eu besoin de connaître la résolution de (E_2), nous aurons ici besoin de connaître la résolution de l'équation diophantienne auxiliaire : $x^2 + 3y^2 = z^3$, résolution qui va maintenant nous occuper un certain temps.

Le lecteur doit certainement connaître l'identité de Diophante $(a^2+b^2)(c^2+d^2)=(ac-bd)^2+(ad+bc)^2$, qui permet d'écrire un produit de deux sommes de deux carrés comme somme de deux itous. Si, dans cette formule, on remplace *b* par $b\sqrt{3}$ et *d* par $d\sqrt{3}$, on obtient :

$$(a^2+3b^2)(c^2+3d^2)=(ac-3bd)^2+3(ad+bc)^2$$

qui montre que les entiers du type x^2+3y^2 sont eux aussi stables par produits.
Une utilisation répétée de cette formule nous donne :

$$(n^2+3m^2)^3=\left((n^2-3m^2)^2+3(2nm)^2\right)(n^2+3m^2)$$

$$=(n^3-9nm^2)^2+3(3n^2m-3m^3)^2$$

Une famille infinie de solutions à l'équation $x^2+3y^2=z^3$ est donc donnée par $x=n^3-9nm^2,\ y=3n^2m-3m^3, n,\ m\in\mathbb{Z}$. Par exemple, *n* = 2 et *m* = 1 donne $10^2+3.9^2=7^3$. Tout le problème est maintenant de savoir si ce sont les seules.
Et c'est là qu'Euler a commis un péché, mais un péché génial. Au lieu de rester sagement dans les entiers bien de chez nous, il est passé dans les nombres complexes. Pour détendre le lecteur avant ces moments terribles, D. Goffinet me conseille le jeu de mot : Euler veut aller dans $\mathbb{C}$, il étend dans $\mathbb{G}$...
Il devait bien savoir (Euler) que la formule :
$(a^2+3b^2)(c^2+3d^2)=(ac-3bd)^2+3(ad+bc)^2$ est une simple transcription (avec les notations actuelles) de : $|z|^2|z'|^2=|zz'|^2$ où $z=a+ib\sqrt{3}$ et $z'=c+id\sqrt{3}$. Et l'équation $x^2+3y^2=z^3$, s'écrit $\left|x+iy\sqrt{3}\right|^2=\left(x+iy\sqrt{3}\right)\left(x-iy\sqrt{3}\right)=z^3$. Or dans les entiers, lorsqu'un produit de 2 termes premiers entre eux est un cube, chacun d'eux est un cube. Euler a froidement étendu cette propriété à l'ensemble des $a+ib\sqrt{3},\ a,\ b\in\mathbb{Z}$, ensemble que l'on note maintenant $\mathbb{Z}\left[i\sqrt{3}\right]$: lorsque *x* et *y* sont premiers entre eux, $x+iy\sqrt{3}$ et $x-iy\sqrt{3}$ également, et leur produit étant un cube, $x+iy\sqrt{3}=\left(n+im\sqrt{3}\right)^3=n^3-9nm^2+i\left(3n^2m-3m^3\right)\sqrt{3}$, d'où
$x=n^3-9nm^2,\ y=3n^2m-3m^3$: on a obtenu l'unicité voulue. Mais Euler a eu de la chance : cette propriété est vraie dans tous les anneaux «factoriels» dans lesquels on a l'unicité de la décomposition en produit de facteurs irréductibles. Or si $\mathbb{Z}\left[i\sqrt{3}\right]$ n'est pas à proprement parler factoriel (car $4=2\times2=\left(1+i\sqrt{3}\right)\left(1-i\sqrt{3}\right)$), il possède une extension factorielle : l'anneau $\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right]=\mathbb{Z}[j]$, anneau des «entiers» sur le corps $\mathbb{Q}\left[i\sqrt{3}\right]$, formé des $\frac{a+ib\sqrt{3}}{2}$, *a*, *b* entiers de même parité.Mais par contre, ni $\mathbb{Z}\left[i\sqrt{5}\right]$, ni l'anneau des entiers de $\mathbb{Q}\left[i\sqrt{5}\right]$, qui lui est égal, ne sont factoriels (car $6=2\times3=\left(1+i\sqrt{5}\right)\left(1-i\sqrt{5}\right)$). La méthode d'Euler ne se généralisera donc pas ... Mais il reste que le théorème de Fermat a été l'initiateur de l'utilisation en arithmétique de ces extensions quadratiques de $\mathbb{Z}$. Pour une étude de ces anneaux, nous renvoyons le lecteur à [Mutafian] pages 248 à 273, par exemple. Et nous considérerons comme démontré le

Lemme 2

Si deux entiers *x* et *y* premiers entre eux sont tels que x^2+3y^2 est un cube z^3, alors il existe deux entiers *n* et *m* premiers entre eux tels que $x+iy\sqrt{3}=\left(n+im\sqrt{3}\right)^3$, ce qui donne : $x=n^3-9nm^2$, $y=3n^2m-3m^3$, $z=n^2+3m^2$.

Bien entendu, on peut arriver à démontrer ce lemme sans le secours des nombres complexes (et Euler était tout à fait en mesure de le faire) ; on trouvera une telle démonstration dans [Weil] et dans [Guinot 3] pages 124 à 126.

Nous pouvons maintenant, en suivant toujours Euler, démontrer le

Théorème 4

L'équation (E_3) : $x^3+y^3=z^3$ n'a pas de solution en entiers non nuls, ou, en français : **la somme de deux cubes non nuls ne peut être un cube**.

Démonstration du théorème 4

► Considérons un solution éventuelle *x*, *y*, *z* à cette équation. La première idée est d'utiliser le fait que $x+y$ divise x^3+y^3, donc z^3. Remarquons auparavant que (E_3), qui peut s'écrire $x^3+y^3+(-z)^3=0$ est symétrique en *x*, *y*, *–z*.. Et comme d'habitude, on se ramène au cas où *x*, *y*, *z* sont deux à deux premiers entre eux. Nous laissons le lecteur voir pourquoi forcément l'un des entiers est pair et les deux autres impairs.

Si, par exemple, *z* est pair (et ceci ne restreint pas la généralité d'après la remarque de symétrie ci-dessus), $u=\frac{x+y}{2}$ et $v=\frac{x-y}{2}$ sont des entiers relatifs non nuls premiers entre eux. Comme $x=u+v$ et $y=u-v$, *u* et *v* sont de parités contraires. L'équation (E_3) devient en *u* et *v* : $2u\left(u^2+3v^2\right)=z^3$.

Si, tout d'abord, *u* n'est pas multiple de 3, on constate facilement que $2u$ et u^2+3v^2 sont premiers entre eux et par conséquent, $2u$ et u^2+3v^2 sont des cubes t^3 et w^3. On voit apparaître l'équation auxiliaire parachutée ci-dessus ! D'après le lemme 2 :

$$u=n^3-9nm^2=n(n-3m)(n+3m),$$

$$v=3n^2m-3m^3=3m(n-m)(n+m),$$

$$w=n^2+3m^2$$

$2n(n-3m)(n+3m)$ est donc un cube ; il reste à vérifier que $2n$, $n–3m$ et $n+3m$ sont deux à deux premiers entre eux. On remarque que puisque *u* et *v* sont premiers entre eux et de parités contraires, *n* et *m* sont premiers entre eux et de parités contraires. D'autre part, *n* n'est pas multiple de 3 car sinon, *u* le serait. Nous laissons le lecteur en déduire lui-même que $2n$, $n-3m$ et $n+3m$ sont deux à deux premiers entre eux, et que ce sont donc des cubes z'^3, x'^3, y'^3 vérifiant $x'^3+y'^3=z'^3$. On a donc retrouvé une solution en entiers non nuls (*x'*, *y'*, *z'*) à (E_3'). Or $|x'y'z'|^3=2|u|=|x+y|$ est un diviseur de $|x^3+y^3|=|z|^3$, donc $|x'y'z'|\le|z|<|xyz|$.

Reste à regarder ce qui se passe si *u* est multiple de 3. dans ce cas, *v* ne l'est pas car *u* et *v* sont premiers entre eux. On écrit alors $u=3w$, d'où $18w\left(v^2+3w^2\right)$ est un cube et l'on

constate encore que $18w$ et v^2+3w^2 sont premiers entre eux donc $18w$ et v^2+3w^2 sont des cubes. De la même façon que ci-dessus, on en déduit une nouvelle solution (x',y', z'') à (E_3'), vérifiant $0<|x'\,y'\,z'|<|xyz|$. Mais ceci est absurde par l'argument de descente infinie. ◄

III Le théorème de Sophie Germain

La démonstration de Dirichlet du cas $n = 5$ du théorème de Fermat nécessite de savoir que l'une des inconnues est divisible par 5, autrement dit d'avoir résolu ce qu'on appelle le premier cas de Fermat. Or cette résolution, faite auparavant par Sophie Germain (dont nous vous recommandons de lire l'étonnante histoire dans [Dahan]), se généralise facilement à une classe plus grande de nombres premiers, c'est pourquoi nous allons l'énoncer dans sa généralité.

Théorème 5, de Sophie Germain

soit p un nombre premier impair tel qu'il existe un nombre premier auxiliaire q vérifiant :

(1) $\forall x,y,z\in Z \quad (x^p+y^p+z^p\equiv 0 \ [q])\Rightarrow(x,y \text{ ou } z\equiv 0 \ [q])$

(2) $\forall x\in Z \quad x^p\neq p \ [q]$

condition vérifiée en particulier si $2p+1$ est un nombre premier.

Alors une solution (x, y, z) de (E_p) est forcément telle que x, y ou z est divisible par p.

Démonstration du théorème 5

► Montrons tout d'abord que si $q = 2p+1$ est un nombre premier, alors q vérifie (1) et (2).

D'après le petit théorème de Fermat, $x^{q-1}=(x^p)^2$ est congru à 0 ou à 1 modulo q, ce qui fait que x^p est congru à 0, 1 ou –1 modulo q ($\mathbb{Z}/q\mathbb{Z}$ est intègre !), donc n'est pas congru à p. Si ni x, ni y, ni z n'est divisible par q, x^p, y^p et z^p sont congrus à ±1 modulo q, et l'on voit que $x^p+y^p+z^p\equiv 0 \ [q]$ est impossible.

Considérons maintenant une solution (primitive comme d'habitude) (x, y, z) de (E_p), dont aucun terme n'est multiple de p, et dans laquelle on a changé z en $-z$ pour raison de symétrie (comme dans le cas 3 ci-dessus). L'égalité $x^p+y^p+z^p=0$ se factorise en $(-x)^p=(y+z)(y^{p-1}-y^{p-2}z+...+z^{p-1})$. Vérifions que les deux facteurs sont premiers entre eux : si un nombre premier r divisait $y + z$ et $y^{p-1}-y^{p-2}z+...+z^{p-1}$, y serait congru à $-z$ modulo r et donc $py^{p-1}\equiv 0 \ [r]$; $r = p$ est impossible car p diviserait $y + z$ donc x, ce qui est supposé ne pas être, donc r divise y : c'est absurde car il diviserait aussi z.

On en déduit que les deux facteurs sont des puissances p-ièmes. Le même raisonnement pouvant être fait sur y et sur z, on obtient, toutes les nouvelles lettres représentant des entiers :

$y+z=a^p$; $y^{p-1}-y^{p-2}z+...+z^{p-1}=\alpha^p$; $x=-a\alpha$

$z+x=b^p$; $z^{p-1}-z^{p-2}x+...+x^{p-1}=\beta^p$; $y=-b\beta$

$x+y=c^p$; $x^{p-1}-x^{p-2}y+...+y^{p-1}=\gamma^p$; $z=-c\gamma$

Travaillons maintenant modulo q : la condition (1) montre que, par exemple, $x\equiv 0$. Donc $2x=b^p+c^p+(-a)^p\equiv 0$, donc (toujours par (1)), a, b ou c est divisible par q. Si b était divisible par q, alors $y=-b\beta$ également ce qui contredirait le fait que x et y sont premiers entre eux. De même pour c, donc c'est a qui est multiple de q. Mais alors $y\equiv -z$, $\alpha^p\equiv py^{p-1}\equiv p\gamma^p$; z n'étant pas multiple de q, γ non plus, et considérons γ' tel que $\gamma\gamma'$ soit congru à 1 ($\mathbb{Z}/q\mathbb{Z}$ est un corps !) ; alors $(\alpha\gamma')^p\equiv p$, ce qui contredit (2). L'un des termes x, y ou z est donc divisible par p. ◄

Les premiers nombres premiers dont le double plus 1 est premier sont : 3, 5, 11, 23, ..., $39051\times 2^{6001}-1$ (Keller, 1986), et ont été baptisés «nombres premiers de Sophie Germain». On ne sait même pas s'il y en a une infinité (le problème est similaire à celui des nombres premiers jumeaux). Mais le théorème fonctionne aussi pour p = 7 ; en effet, si $2p+1$ = 15 n'est pas premier, q = $4p+1$ = 29 l'est ; x^{4p} est congru à 0 ou 1 modulo q, donc x^p est congru à 0, ±1 ou ±12 (12 est racine carrée de –1 modulo 29), et l'on a bien (1) et (2). D'ailleurs, Legendre a montré que si p est un nombre premier tel que $4p+1$, $8p+1$, $10p+1$, $14p+1$ ou $16p+1$ est premier, alors le premier cas de Fermat est réalisé pour p.

IV Le cas *n* = 5.

Nous terminerons cet article par la démonstration de Dirichlet, qui complète celle de Sophie Germain. Cette démonstration est, en plus long et plus méticuleux, du même type que celle d'Euler pour le cas 3. Cependant, la descente infinie ne sera pas du même genre que les précédentes : au lieu d'aboutir à une solution plus «petite» de l'équation de départ, on va construire une suite auxiliaire d'entiers, strictement décroissante et infinie, ce qui sera le point absurde. D'autre part, l'équation annexe à résoudre sera ici du type $x^2-5y^2=z^5$, ce qui nous entraînera dans l'anneau $\mathbb{Z}\left[\sqrt{5}\right]$ (car $x^2-5y^2=\left(x+y\sqrt{5}\right)\left(x-y\sqrt{5}\right)$). Or, contrairement à ce que dit [Devlin] page 167, il se produit un phénomène similaire à celui qui s'est produit avec $\mathbb{Z}\left[i\sqrt{3}\right]$: $\mathbb{Z}\left[\sqrt{5}\right]$ n'est pas factoriel (car $4=2\times 2=\left(-1+\sqrt{5}\right)\left(1+\sqrt{5}\right)$), mais il possède une extension factorielle : l'anneau $\mathbb{Z}[\varphi]$ (où $\varphi=\frac{1+\sqrt{5}}{2}$ est le nombre d'or), anneau des «entiers» sur le corps $\mathbb{Q}\left[\sqrt{5}\right]$, formé des $\frac{a+b\sqrt{5}}{2}$, a, b entiers de même parité.

Nous aurons besoin des 2 lemmes suivants.

Lemme 3

Si deux entiers *x* et *y* premiers entre eux, *y* multiple de 5, sont tels que x^2-5y^2 est une puissance cinquième d'entier z^5, alors il existe deux entiers *n* et *m* premiers entre eux de parités contraires tels que $x+y\sqrt{5}=\left(n+m\sqrt{5}\right)^5$, ce

qui donne : $\boxed{x = n^5 + 50n^3m^2 + 125nm^4,\ y = 5n^4m + 50n^2m^3 + 25m^5}$, $\boxed{z = n^2 - 5m^2}$.

Lemme 3'

Si deux entiers *x* et *y* impairs premiers entre eux, *y* multiple de 5, sont tels que $\boxed{\left(\frac{x}{2}\right)^2 - 5\left(\frac{y}{2}\right)^2}$ **est une puissance cinquième d'entier** $\boxed{z^5}$**, alors il existe deux entiers *n* et *m* impairs premiers entre eux tels que** $\boxed{\frac{x}{2} + \frac{y}{2}\sqrt{5} = \left(\frac{n}{2} + \frac{m}{2}\sqrt{5}\right)^5}$**, ce qui donne :**

$\boxed{16x = n^5 + 50n^3m^2 + 125nm^4,\ 16y = 5n^4m + 50n^2m^3 + 25m^5}$, $\boxed{4z = n^2 - 5m^2}$.

Ces deux lemmes très délicats sont démontrés directement dans [Edwards] pages 68 et 72. La démonstration de la factorialité de $\mathbb{Z}[\varphi]$ se trouve dans [Hardy & Wright] page 214 (il s'agit de démontrer que la «norme», définie par $N(u + v\sqrt{5}) = u^2 - 5v^2$ est «euclidienne» dans $\mathbb{Z}[\varphi]$, c'est-à-dire si *a* et *b* sont deux éléments non nuls quelconques de $\mathbb{Z}[\varphi]$, il existe *q* et *r* dans $\mathbb{Z}[\varphi]$ tels que $a = bq + r$ avec $|N(r)| < |N(b)|$).

Lemme 4

il est impossible de trouver 4 entiers *n*, *m*, *c* et *d* (*n* et *m* non nuls premiers entre eux de parités contraires), tels que

$$\boxed{\begin{aligned} 5^4.2m &= c^5 \\ n^4 + 10n^2m^2 + 5m^4 &= d^5 \end{aligned}}$$

Démonstration du lemme 4.

► La première égalité montre que *m* est multiple de 5, et la deuxième peut s'écrire $a^2 - 5b^2 = d^5$ où $a = n^2 + 5m^2$ et $b = 2m^2$; a et b sont premiers entre eux car si un nombre premier divisait *a* et *b*, il diviserait $2a - 5b = 2n^2$ et $2m^2$, ce serait donc 2 mais c'est impossible car *a* est impair ; *b* étant divisible par 5, une application du lemme 3 donne $\boxed{a = p^5 + 50p^3q^2 + 125pq^4,\ b = 5p^4q + 50p^2q^3 + 25q^5}$ où *p* et *q* sont premiers entre eux et de parités contraires (car si p et q étaient impairs, *a* serait pair). L'on obtient :

$$5^5.5^4.2q\left(p^4 + 10p^2q^2 + 5q^4\right) = 5^8.2b = 5^8.2^2m^2 = c^{10}$$

L'on vérifie que $5^4.2q$ et $p^4 + 10p^2q^2 + 5q^4$ sont premiers entre eux : il est clair qu'un nombre premier diviseur commun ne peut être que 2 ou 5 ; 2 est impossible car $p^4 + 5q^4$ serait pair, et 5 non plus car *p* serait multiple de 5, donc *a* aussi, comme *b*. L'on peut donc écrire :

$$\boxed{\begin{aligned} 5^4.2q &= e^5 \\ p^4 + 10p^2q^2 + 5q^4 &= f^5 \end{aligned}}$$

encadré qui a un net air de famille avec celui de départ. Or $\boxed{b = 2m^2 = q\left(5p^4 + 50p^2q^2 + 25q^4\right)}$ montre que $q > 0$ et $2m^2 > 25q^4$, d'où $m > q > 0$. Ceci est absurde par l'argument de descente infinie. ◄

Lemme 4'

il est impossible de trouver 4 entiers *n*, *m*, *c* et *d*, *n* et *m* impairs premiers entre eux, tels que

$$\boxed{\begin{aligned} 5^4 m &= c^5 \\ n^4 + 10n^2m^2 + 5m^4 &= 2^4 d^5 \end{aligned}}$$

Démonstration du lemme 4'.

► La première égalité montre que *m* est multiple de 5, et la deuxième peut s'écrire $\left(\frac{a}{2}\right)^2 - 5\left(\frac{b}{2}\right)^2 = d^5$ où $a = \frac{n^2 + 5m^2}{2}$ et $b = m^2$; *a* et *b* sont premiers entre eux car si un nombre premier divisait *a* et *b*, il diviserait $2a - 5b = n^2$ et m^2, ce qui est impossible. On vérifie également qu'ils sont impairs ; *b* étant divisible par 5, une application du lemme 3' donne $\boxed{16a = p^5 + 50p^3q^2 + 125pq^4,\ 16b = 5p^4q + 50p^2q^3 + 25q^5}$ où *p* et *q* sont premiers entre eux impairs. L'on obtient :

$$5^5.5^4 q\frac{p^4 + 10p^2q^2 + 5q^4}{16} = 5^8 b = 5^8 m^2 = c^{10}$$

L'on vérifie alors que $5^4 q$ et $\frac{p^4 + 10p^2q^2 + 5q^4}{16}$ sont premiers entre eux et l'on peut donc écrire :

$$\boxed{\begin{aligned} 5^4 q &= e^5 \\ p^4 + 10p^2q^2 + 5q^4 &= 16f^5 \end{aligned}}$$

encadré qui a lui aussi un net air de famille avec celui de départ. Or $\boxed{16b = 16m^2 = q\left(5p^4 + 50p^2q^2 + 25q^4\right)}$ montre que $q > 0$ et $16m^2 > 25q^4$, d'où $m > q > 0$. Ceci est absurde par l'argument de descente infinie. ◄

Nous pouvons passer à la démonstration générale :

Théorème 6

l'équation (E_5) : $\boxed{x^5 + y^5 = z^5}$ n'a pas de solution en entiers non nuls, ou, en français : **la somme de deux puissances cinquièmes d'entiers non nuls ne peut être une puissance cinquième d'entier**.

Démonstration du théorème 6.

► D'après le théorème de Sophie Germain, l'un des termes d'une solution en entiers non nuls, primitive, (*x*, *y*, *z*) de (E_5), est divisible par 5, et l'on ne restreint pas la généralité en supposant que c'est *z*. Nous allons maintenant faire deux raisonnements suivant que *z* est pair ou non (le premier raisonnement est dû à Dirichlet, et le deuxième à Legendre, mais à nouveau simplifié par Dirichlet).

Lorsque *z* est pair, *x* et *y* sont impairs et $u = \frac{x+y}{2}$, $v = \frac{x-y}{2}$ sont entiers premiers entre eux, de parités contraires. L'équation (E_5) devient alors : $2u\left(u^4 + 10u^2v^2 + 5v^4\right) = z^5$. Si le premier facteur avait été $5^4.2v$ au lieu de $2u$, le lemme 4 nous aurait permis de

conclure aussitôt. Mais le fait que 5 divise z (voilà pourquoi le théorème de Sophie Germain est indispensable) va nous permettre de nous y ramener. Comme 5 divise $u\left(u^4+10u^2v^2+5v^4\right)$, il divise *u* ou u^4 : *u* est donc multiple de 5. Posant *u* = *5w*, on obtient : $50w\left(v^4+50v^2w^2+125w^4\right)=z^5$. Les deux facteurs étant premiers entre eux, on obtient :

$$50w=a^5$$

$$v^4+50v^2w^2+125w^4=b^5$$

Ce n'est pas encore tout à fait comme la forme du lemme 4, mais on va y parvenir. La deuxième égalité peut se mettre sous la forme $V^2-5W^2=b^5$ où $V=v^2+25w^2$ et $W=10w^2$ sont premiers entre eux. W étant divisible par 5, le lemme 3 montre qu'il existe *n* et *m* premiers entre eux de parités contraires tels que $\boxed{V=n^5+50n^3m^2+125nm^4,\ W=5n^4m+50n^2m^3+25m^5}$. L'on obtient :

$$5^4.2m\left(n^4+10n^2m^2+5m^4\right)=5^3.2W=5^4.2^2w^2=a^{10}.$$

Les deux facteurs étant premiers entre eux, on obtient :

$$\boxed{\begin{aligned}&5^4.2m=c^5\\&n^4+10n^2m^2+5m^4=d^5\end{aligned}}$$

ce qui est impossible par le lemme 4.

Lorsque *z* est impair, *x* et *y* sont de parités contraires et l'on posé *u* = *x* + *y*, v = *x* - *y* au lieu de $u=\frac{x+y}{2}$, $v=\frac{x-y}{2}$ précédemment ; *u* et *v* sont alors impairs premiers entre eux. L'équation (E_5) devient alors : $u\left(u^4+10u^2v^2+5v^4\right)=16z^5$.

Comme 5 divise *z*, 5 divise $u\left(u^4+10u^2v^2+5v^4\right)$ et il divise *u* ou u^4 : *u* est donc multiple de 5. Posant *u* = *5w*, on obtient : $25w\left(v^4+50v^2w^2+125w^4\right)=16z^5$. Les deux facteurs étant premiers entre eux et le premier impair, on obtient :

$$25w=a^5$$

$$\left(v^2+25w^2\right)^2-5\left(10w^2\right)^2=16b^5$$

Le carré d'un nombre impair étant congru à 1 modulo 8, v^2+25w^2 est congru à 2 : il est donc pair, non multiple de 4. les entiers $V=\frac{v^2+25w^2}{2}$ et $W=5w^2$ sont donc impairs (premiers entre eux) et vérifient : $\left(\frac{V}{2}\right)^2-5\left(\frac{W}{2}\right)^2=b^5$. W étant divisible par 5, le lemme 3' montre qu'il existe *n* et *m* impairs (premiers entre eux) tels que $\frac{V}{2}+\frac{W}{2}\sqrt{5}=\left(\frac{n}{2}+\frac{m}{2}\sqrt{5}\right)^5$. Si l'on tire la valeur de W en *n* et *m*, l'on obtient : $5^4m\left(n^4+10n^2m^2+5m^4\right)=16.5^3W=16a^{10}$. Les deux facteurs étant premiers entre eux, on obtient encore une fois :

$$5^4m=c^5$$

$$n^4+10n^2m^2+5m^4=16d^5$$

Ceci est impossible par le lemme 4' ◄

Voilà donc où on en était en 1825. La complexité des démonstrations ci-dessus nous montre bien que d'autres voies et d'autres outils devaient être créés pour tordre le coup au cas général. Mais la route fut longue et difficile : dans le livre de [Noguès] qui fait le point des connaissances en 1931, ce que nous venons de faire tient en 4 pages sur 150 ! Nous ne savons pas sur combien de pages tiendraient les années postérieures à 1931, mais nous savons maintenant que ce nombre est fini.

Bibliographie

- concernant exclusivement le théorème de Fermat.

[Edwards] H. M. Edwards : Fermat's last theorem (Springer Verlag, 1977).
[Noguès] R. Noguès : théorème de Fermat , son histoire (Vuibert, 1932 ; A. Blanchard, 1966 ; J. Gabay, 1992)
[Ribenboim] P. Ribenboim : 13 lectures on Fermat's theorem (Springer Verlag, 1980). La première de ces «lectures» a été traduite dans la brochure de l'APMEP n° 41, fragments d'histoires des mathématiques, (1981), pages 99 à 120.

- évoquant le théorème de Fermat ou cité dans l'article.

[Cuculière] R. Cuculière : mille ans de chasse aux nombres congruents, Pour la Science, juillet 1987, pages 14 à 18.
[Dahan] A. Dahan Dalmedico : Sophie Germain, Pour la Science, octobre 1988, pages 36 à 45.
[Devlin] K. Devlin : mathématiques, un nouvel âge d'or, pages 157 à 176 (Masson, 1992).
[Guinot 1] M. Guinot : Pythagore, Euclide et toute la clique (Aléas, 1992).
[Guinot 2] M. Guinot : les resveries de Fermat , pages 101 à 109 (Aléas, 1993).
[Guinot 3] M. Guinot : ce diable d'homme d'Euler, pages 129 à 134 (Aléas, 1994).
[Hardy & Wright] G. H. Hardy, E. M. Wright : an introduction to the theory of numbers (Oxford university press, 1938)
[Itard] J. Itard : arithmétique et théorie des nombres, pages 106 à 117 (PUF, Que-sais-je ?, 1963).
[Mutafian] C. Mutafian : le défi algébrique, tome 2 (Vuibert, 1976).
[Stewart] I. Stewart : voyage au pays de Fermat, Pour la Science, mars 1989, pages 102 à 107.
[Universalis] M. David, J. L. Coliot - Thélène : article sur les équations diophantiennes dans l'encyclopédie Universalis.
[Weil] A. Weil, number theory, an approach through history, from Hammurapi to Legendre (Birkhäuser, 1983).