HISTOIRE DU DERNIER THEOREME DE FERMAT

Hervé Stève,
herve.steve@hotmail.fr

Kafemath du 16 juillet 2020

À la Coulée Douce, Paris 12ème

Sommaire

- ✓ **Introduction**
- ✓ **Triplets pythagoriciens**
- ✓ **De Fermat à Kummer**
- ✓ **Preuve d'Andrew Wiles**

Bibliographie :

- *Arithmetica* de Diophante d'Alexandrie (IIIème siècle), avec annotations de Pierre de Fermat publié en 1670
- *Modular Elliptic Curves and Fermat's Last Theorem* (1995) d'Andrew Wiles, Annals of Mathematics (109 pages) article en ligne
- *Le dernier théorème de Fermat* de Simon Singh (1999)

a

l'énoncé

Le dernier théorème de Fermat :
pas de solutions entières non nulles pour l'équation

$x^n + y^n = z^n$ pour n>2

Est appelé aussi

- *Le grand théorème de Fermat*,
- *La conjecture de Fermat* avant sa preuve puis
- *Le théorème de Fermat-Wiles* depuis 1994

- Le cas n=0 : 1 + 1 = 1 , impossible
- Le cas n=1 : x + y = z , addition des entiers
- Le cas n=2 avec les **triplets pythagoriciens** (Antiquité) ex) $3^2 + 4^2 = 5^2$

- Le cas n < 0 : se ramène à Fermat avec x',y',z' tq x'=yz, y'=zx, z'=xy
- Pour n=-1 , 1/3 + 1/6 =1/2 ; pour n=-2 : $1/20^2 + 1/15^2 = 1/12^2$

a

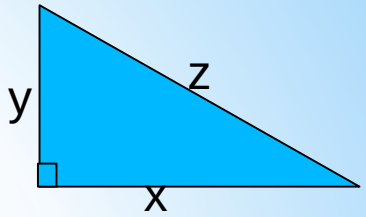
Chronologie de la preuve

- **Pierre de Fermat** pose le problème, prétend l'avoir résolu (1670). **Euler** (1753) termine la preuve pour n=4 et s'attaque au cas n=3 : **Gauss** termine la démonstration (1801).

- **Sophie Germain** (1804) démontre le théorème qui porte son nom, puis en 1825 démontre le théorème de Fermat pour des n premiers < 100
- 1825 : Lejeune Dirichlet et Adrien-Marie Legendre prouvent n=5. Legendre tente la généralisation à partir du théorème de Sophie Germain. Lamé démontre n=7 en 1839. En 1847 : Lamé et Cauchy échouent pour la démonstration générale
- 1847 : **Ernst Kummer** démontre le théorème de Fermat pour n premier régulier …
- De 1850 à 1969 : de nouvelles avancées pour des valeurs de n
- À partir de 1952 : des démonstrations prouvées sur l'ordinateur pour n<2000 …

- À partir des années 1960, les travaux sur les courbes elliptiques et les fonctions modulaires préparent la preuve d'**Andrew Wiles en 1994** : il démontre une conjecture plus faible que celle de **Shimura-Taniyama-Weil** qui implique alors le dernier théorème

Triplets pythagoriciens



Cas n=2 : solutions entières de la relation de Pythagore $x^2 + y^2 = z^2$, z diagonale ou hypoténuse

- **Tablette babylonienne Plimpton 322** (-1800 a.j.c.)

en cunéiforme de 15 lignes sur 4 colonnes

Ex) *ligne 1 on lit en base 60 (1:)59:00:15 1:59 2:49 1*

x=1x60+59=119 , z=2x60+49=169 d'où y=120

- Éléments d'Euclide : livre X vers -300 a.j.c.

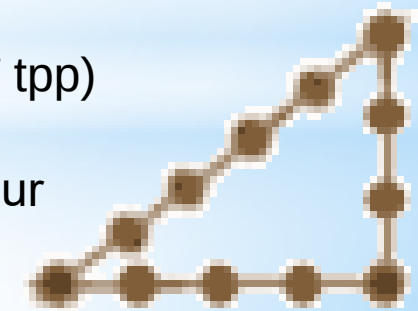
Triplets pythagoriciens primitifs (tpp) : x, y, z sont premiers entre eux (pas de diviseurs communs)

Si (x,y,z) tpp alors x impair est équivalent à l'existence de p, q premiers entre eux p>q>0 tq $x=p^2-q^2$, $y=2pq$ et $z=p^2+q^2$

On obtient ainsi une infinité de tpp !

- Exemple célèbre) x=3, y=4 et z=5 dit **triangle égyptien** (1er tpp)

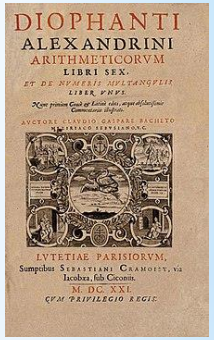
Application : corde à nœuds de longueur 12 coudées pour la construction dans le bâtiment (cathédrales, forteresses, …) pour respecter les proportions.



Pierre de Fermat

Magistrat (Bordeaux, Toulouse), mathématicien « amateur »
Naissance vers 1605, mort en 1665
Notes publiées par son fils en 1670

- Fermat constate que si il y a une infinité de solutions entières non triviales de $x^n+y^n=z^n$ pour n=2 (triplets pythagoriciens), personne n'en a trouvé pour les cubes. Il écrit dans la marge de ***Arithmetica*** **de Diophante** qu'il a une preuve « véritablement merveilleuse » pour tout n>2 mais ne l'a pas écrite par manque de place …



- mais il fournit une preuve « incomplète » du cas n=4 à partir du

Théorème sur les triangles rectangles :
Si x,y,z entiers tq $x^2 + y^2 = z^2$ avec l'aire $A=xy/2=d^2$ alors d ne peut être entier

<u>Démonstration par l'absurde avec la méthode de descente infinie :</u>
- Supposons que $A=xy/2=(p^2-q^2)pq$ soit un carré parfait. S'il existait une aire B de carré parfait plus petit alors ce serait impossible car B est un entier positif.
- Comme p, q, p-q, p+q sont premiers entre eux alors ils sont tous des carrés. Soient $r^2=p-q$, $s^2=p+q$ avec r, s impairs, $u=(r-s)/2$ et $v=(r+s)/2$, alors $u^2+v^2=p$ est un carré d'un nouveau triangle pythagoricien d'aire $B=uv/2=q/4$ d'où B carré < A . CQFD

Remarque : le théorème sur les triangles rectangles est équivalent au problème $x^4 – y^4 = z^2$ c.à.d. un corolaire du cas n=4 du dernier théorème (voir Euler pour une preuve complète)

a

Leonhard Euler

Mathématicien et physicien suisse
Naissance vers 1707, mort en 1783

- **Cas n=4** : démonstration complète et plus simple sur $x^4+y^4=z^2$ (1738)

Preuve par l'absurde :

- si il y a une solution, alors (x^2,y^2,z) est un tpp i.e. $x^2=p^2-q^2$, $y^2=2pq$ et $z^2=p^2+q^2$
- de même, comme (x,q,p) est un tpp, on a $x=m^2-n^2$, $q=2mn$ et $p=m^2+n^2$
- comme p et 2q premiers entre eux donc ils sont des carrés
- alors $2q=4mn$ est un carré et aussi m et n : donc il existe (x',y',z') tq $m=x'^2$, $n=y'^2$ et $p=z'^2$ d'où $m^2+n^2=x'^4+y'^4=z'^2$
- Comme $z'^2=p < z^2$ c'est impossible d'après la méthode de descente infinie. CQFD

- **Cas n=3** : en 1753, Euler étudie $z^3=x^3+y^3=2p(p^2+3q^2)$ avec $p=(x+y)/2$ et $q=(x-y)/2$ premiers entre eux. Preuve publiée en 1770 mais incomplète

- Euler introduit les nombres complexes et décompose $p^2+3q^2=(p+i\sqrt{3}q)(p-i\sqrt{3}q)$ avec $i^2=-1$. Si p^2+3q^2 est un cube, $p+i\sqrt{3}q$ et $p-i\sqrt{3}q$ aussi car ils premiers entre eux …
- mais la décomposition dans $Z(a+ib\sqrt{3})$ avec a, b entiers dans Z n'est toujours pas unique.

exemple) a=b=1 : $1 + 3 = 2 \times 2 = (1+i\sqrt{3})(1-i\sqrt{3})$ *Euler veut aller dans C mais il est (en) dans G* !*

- **Remarque** : $6^3 + 8^3 = 9^3 - 1$, la somme de 3 cubes est bien un cube

Euler conjecture que $x^n + y^n + z^n = t^n$ n'a pas de solutions pour n>3

Mais Noam Elkies en 1987 trouve $95\,800^4 + 217\,519^4 + 414\,560^4 = 422\,481^4$

(*) d'après D. Goffinet

Carl Friedrich Gauss

Mathématicien et astronome allemand
Naissance vers 1777, mort en 1855

- **Cas n=3 :** vers 1801, cherche à résoudre dans Z entiers relatifs :

$x^3+y^3+z^3=0$ (z en -z)

Gauss reprend la démonstration d'Euler dans l'anneau Z(a+jb) entiers d'Eisenstien avec $j=(1\pm i\sqrt{3})/2$. Il prouve par l'absurde avec la méthode de descente infinie, qu'il n'y a pas de solutions dans Z(a+jb) et donc dans Z (b=0)

- **Entiers quadratiques** : $Z(a+\omega b)$ avec ω complexe tq $\omega^2 = n+\omega m$ avec n,m dans Z

<u>4 Propriétés</u> :

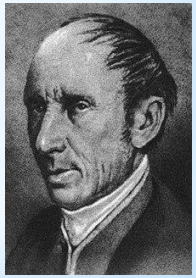
(i) anneau commutatif : groupe abélien pour + , 1 x = x 1= x et x y = y x
(ii) intègre : x y = 0 => x=0 ou y=0
(iii) factoriel : si x non nul et non inversible alors x produit de nombres premiers dans $Z(a+\omega b)$
(iv) tout élément inversible a une racine n-ième : $x^n=y$

- Dans Z (ω=0) : seulement 2 racines de l'unité 1 et -1 …
- Z(a+bj) permet de résoudre le cas n=3 (Gauss)
- $Z(a+b\Phi)$ avec $\Phi=(1+\sqrt{5})/2$ nombre d'Or permet de résoudre le cas n=5 (Legendre et Dirichlet)
- Le cas n=7 a été résolu par Lamé

Pas de généralisation car les anneaux $Z(a+\omega b)$ ne sont pas toujours factoriels …

Bilan intermédiaire

- Si (x,y,z) solution de $x^n + y^n = z^n$ alors (ax,ay,az) est aussi solution
- Si (x,y,z) solution alors le PGCD de 2 entiers est diviseur du $3^{ème}$, ce qui permet de restreindre les solutions …
- Comme le cas n=4 (traité par Fermat et Euler) n'a de solutions alors les cas n=4 x 2^k n'en pas aussi.
- Fermat remarque que si $x^p + y^p = z^p$ n'a pas de solutions alors $(x^q)^p + (y^q)^p = (z^q)^p$ n'en a pas aussi : ce qui revient à ne traiter que les cas n premiers …
- On a vu que les cas n=3, 5 et 7 ont été résolus , il reste donc :
  n = 11, 13, 17, 19, 23, 29, 31, 37, … , 97, 101, … **soit 21 cas < 100** !
- Anneaux des polynômes de Augustin Louis Cauchy (1847) :
  soient (p,q,r) 3 polynômes complexes et n>2 , si $p^n + q^n = r^n$ et si p,q premiers entre eux alors les p,q,r sont constants. Résolutions plus simples car dans l'anneau des polynômes complexes, les éléments inversibles ont une racine n-ième … mais Cauchy ne résout pas de nouveaux cas !



a

Sophie Germain

1ère mathématicienne française, physicienne et philosophe
Naissance 1776, morte en 1831 (cimetière Père Lachaise)

- À partir de 1804, elle correspond avec Gauss sous le nom d'Antoine Auguste Le Blanc

Théorème de Sophie Germain*:

Soit p>2 premier, il existe q premier vérifiant : (i) 2 classes modulo q consécutives non nulles ne peuvent être simultanément des puissances $p^{ième}$, (ii) p lui même (modulo q) n'est pas une puissance $p^{ième}$. Alors si 3 entiers x, y, z vérifient $x^p+y^p=z^p$, l'un au moins est divisible par p^2.

- En 1825, Sophie Germain introduit G** **nombre premier de Sophie Germain** si q=2G+1 est premier aussi. Alors le théorème de Sophie Germain implique qu'il n'existe pas x, y, z entiers tq xyz non divisible par G>2 et $x^G+y^G=z^G$, et ainsi le dernier théorème de Fermat est vrai pour : G=3, 5, 11, 23, 29, 41, 53, 83, 113, …

- Le théorème s'étend à q=2Np+1 avec N entier :

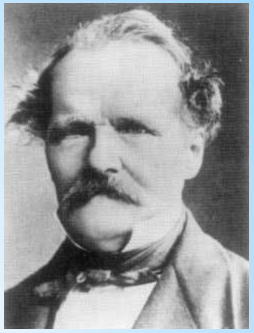
Exemple) p=7 , q=2*7+1=3x5 pas premier mais q=2*2*7+1=29 l'est !
p=13, q=2*13+1=3*9 pas premier mais q=2*2*13+1=53 l'est !
Mais comme les nombres q sont limités … la généralisation échoue

- **Conjecture** : Les nombres premiers de Sophie Germain sont en nombre infini

a

(*) théorie des nombres de Legendre

Ernst Kummer



Mathématicien allemand
Naissance 1810, mort en 1893

- Il démontre en 1847 le théorème de Fermat pour tout **entier premier régulier**

Pour n>2, un nombre p premier régulier s'il ne divise pas le nombre de classes de l'anneau $Z(a+\zeta_p b)$ avec $\zeta_p = \exp(2i\pi/p)$ racines p-ième de X^p-1.

Kummer factorise $x^p + y^p = z^p$ en $(x+ \zeta_p^0 y)(x+ \zeta_p^1 y)\ldots(x+ \zeta_p^{p-1} y)= z^p$
Les facteurs $(x+ \zeta_p^i y)$ sont premiers entre eux (anneaux des idéaux) et aboutit au théorème par contradiction

- En pratique, p est premier régulier si et seulement p^2 ne divise aucune des sommes $S_k(p)=1^k + 2^k + 3^k + \ldots + (p-1)^k$ pour k=2, 4, 6,…, p-3

En 1874, Kummer prouve le théorème de Fermat sauf pour **37, 59, 67**, 101, 103, 131, 149, 157 … **soit 3 nombres irréguliers < 100 !**

p=3 premier régulier (pas de test), $\zeta_3 = \exp(2i\pi/3)=j$
p=5 premier régulier car $S_2(5)=1^2+2^2+3^2+4^2=30$ ne divise pas 25
p=13 premier pas SG mais régulier car $S_2(13)=650$, $S_4(13)=60170$, $S_6(13)=6735950$, $S_8(13)=812071910$, $S_{10}(13)=102769130750$ ne divisent pas 169
p=37 premier irrégulier car $S_{32}(37)\sim1{,}05\ldots10^{+50}$ divise 1369 (p=59 aussi avec S_{44} et p=67 avec S_{58})

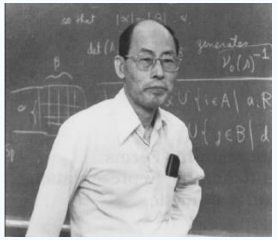
- Les nombres premiers de Sophie Germain sont réguliers. On ne sait pas si les nombres premiers réguliers sont en nombre infini (conjecture), par contre, les irréguliers le sont bien (Jensen 1915) : dommage !

a

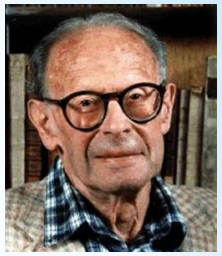
Conjecture de modularité (STW)

Yutaka Taniyama 1927-1958

Goro Shimura 1930-2019



André Weil 1906-1998



- En 1955 à Tokyo, les 2 japonais énoncent une conjecture établissant un pont entre l'arithmétique et la géométrie :

Toute courbe elliptique rationnelle est modulaire i.e. E ≡ M

E courbes elliptiques rationnelles : $Y^2 = X^3 + a X + b$, équations cubiques

M formes modulaires : surfaces « symétriques » associées à une fonction modulaire $f(q)=\Sigma_{n\geq 1}\ a_n\ q^n$ avec a_n points de E à coordonnées entières

- En 1972, Yves Hellegouarch transforme $x^n + y^n = z^n$ en une cubique d'équation :

$Y^2 = X\ (X - x^n)\ (X + y^n)$ avec x,y entiers >0.

Gerhard Frey en 1984 remarque que cette cubique ne semble pas modulaire !

Jean-Pierre Serre en 1985 énonce alors la conjecture epsilon :

si la conjecture de Fermat est fausse alors il existe une courbe elliptique rationnelle semi stable non modulaire …

on a donc 3 conjectures … mais … un lien avec Fermat !

Courbes elliptiques

- Équations cubiques (de Weierstrass) :

  $Y^2 = X^3 + a\,X + b$

  (Loi de groupe sur les points).

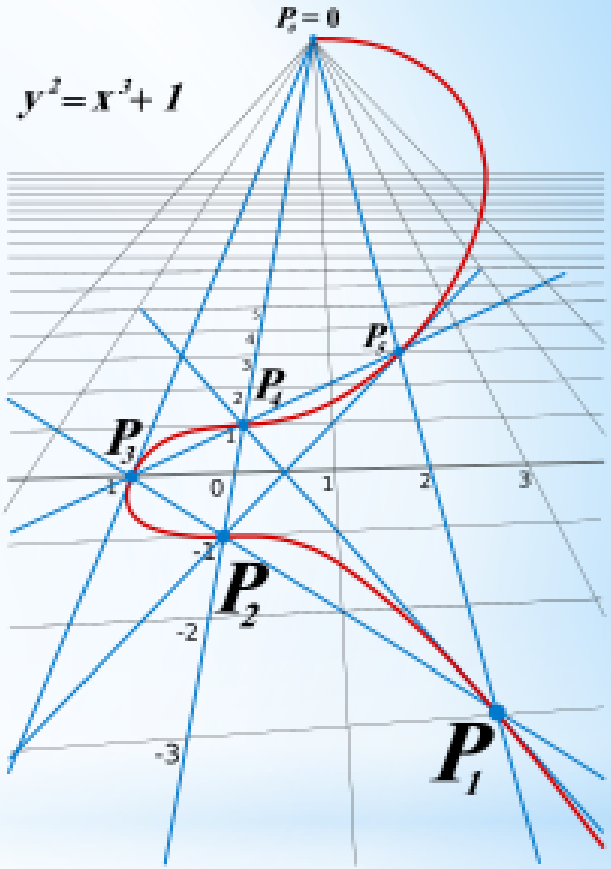
- Recherche de solutions entières sur les groupes cycliques Z/nZ (thèse de doctorat d'Andrew Wiles)

- Par exemple pour la cubique $y^2 + y = x^3 - x^2$

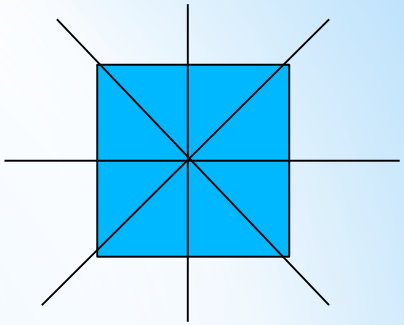
Dans Z, il n'est pas facile de trouver toutes les solutions

Dans Z/5Z, on trouve l'ensemble E_5={(0,0),(0,4),(1,0),(1,4)} ayant 4 solutions

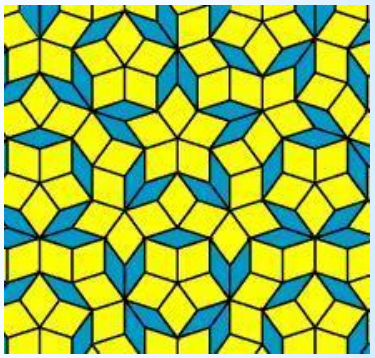
On obtient une suite de nombres de solutions $\#E_n$ (cardinal de E) qui caractérise la courbe elliptique :
$\#E_1$=1, $\#E_2$=4, $\#E_3$=4, $\#E_4$=8, $\#E_5$=4, $\#E_6$=16, $\#E_7$=9, $\#E_8$=16, … **soit l'ADN de la courbe elliptique**



Formes modulaires

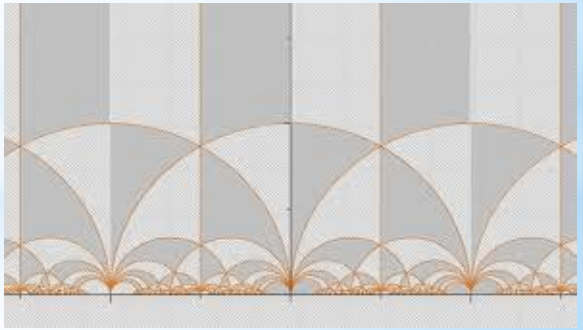


- sur un carré, il y a des **symétries** de rotation (1/4 de tour, demi tour, ¾ de tour, tour entier) et de réflectivité (4 transformations selon les 2 axes centraux et les 2 diagonales) qui laissent le carré identique. Sur un espace pavé de carrés, on obtient aussi des symétrie de translations selon 2 axes



- D'autres pavages dans le plan (x,y) sont plus complexes : ceux de Roger Penrose avec 2 types de forme mais ils ne possèdent pas de symétrie. Par contre, les formes modulaires peuvent en posséder une infinité car elles sont dans espaces à 4 dimensions dans le plan hypercomplexe (xr,xi,yr,yi) avec xr,yr parties réelles et xi,yi parties imaginaires

- A chaque forme modulaire M_n on peut définir le nombre de types de forme qu'elles contiennent. On établit une nouvelle suite de nombres de types de forme $\#M_n$ (cardinal de M) qui caractérise la forme modulaire soit **l'ADN de la forme modulaire**



- Ex) la courbe elliptique $y^2 - y = x^3 - x^2$ est associée à une forme modulaire primitive $f(q) = q - 2q^2 - q^3 + 2q^4 + q^5 + q^6 + \ldots$

Démonstrations des conjectures

- En 1986, Ken Ribet démontre la conjecture epsilon.

Si Fermat est faux alors la conjecture STW est fausse, mais par contraposée :

si la conjecture STW est vraie alors la conjecture de Fermat est vraie

- Cependant si une courbe elliptique rationnelle semi stable est modulaire alors la conjecture de Fermat est vraie.

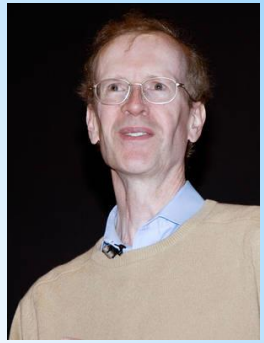
Andrew Wiles démontre cette conjecture entre 1987 et 1994 :

Toute courbe elliptique E rationnelle semi stable est modulaire M i.e.
$E(k) \equiv M(k)$, $k>0$

- La conjecture modulaire STW est prouvée en 1999 par Christophe Breuil, Briand Conrad, Fred Diamond et Richard Taylor

a

Preuve d'Andrew Wiles



Mathématicien britannique né en 1953 à Cambridge, UK

- 7 ans de travaux : au bout d'un an, il décide de procéder par récurrence
- Initialisation (2 ans) : on démontre k=1 i.e. E(1) ≡ M(1). Théorie des **groupes de Galois** appliquée aux courbes elliptiques et aux fonctions modulaires
- Induction : on suppose vrai pour k, on démontre k+1. Méthode d'analyse des courbes elliptiques : la **théorie d'Iwasawa** mène à une impasse fin 1991 ! La nouvelle **méthode de Kolyvagin-Flach** permet à Wiles d'aller au bout de la démonstration. Il fait vérifier son travail auprès de Nick Katz (Université de Princeton).
- Exposé historique en juin 1993 au Isaac Institute (Cambridge, UK). La preuve manuscrite est soumise à un jury mais il reste « un petit problème » sur l'emploi de la méthode de Kolyvagin-Flach (chapitre 3/6 soumis à Nick Katz) « le système d'Euler ne peut être appliqué » !
- 14 mois plus tard alors qu'il travaille avec Richard Taylor, Andrew Wiles décide de compléter la méthode de Kolyvagin-Flach par celle d'Iwasawa … et ça marche enfin !
- Le 17 juin 1995, la preuve est entérinée à Paris : le prix Fermat de l'Académie des Sciences de 1850 lui est remis. Le prix Wolfskhel de 1908 (50 000$) est aussi remis, le prix Abel en 2016 …

Conclusion

- Un **énoncé simple** au départ !
- Mais des **démonstrations difficiles**, subtiles, complexes, beaucoup d'erreurs … impliquant des mathématiciens amateurs et professionnels du monde entier pendant 350 ans !
- **Pont entre l'arithmétique et la géométrie,** grâce à STW
- Nombreuses théories employées, méthodes, analyses, … , le dernier théorème (a) fait **progresser les mathématiques**
- En 2008 : une autre preuve du théorème par Khare-Wintemberger (conjecture de modularité de Jean-Pierre Serre)
- Des **questions encore ouvertes** : Peut-on se passer de STW ? Si oui, Fermat avait-il la démonstration ?
- Science Fiction : dans Star Trek saison 2 épisode 12 en 1989, le dernier théorème est démontré au 24ème siècle ! Mais saison 3 épisode 25 en 1995, une nouvelle démonstration originale est découverte au 23ème siècle !

a

MC Escher
Cercle limite IV ciel enfer