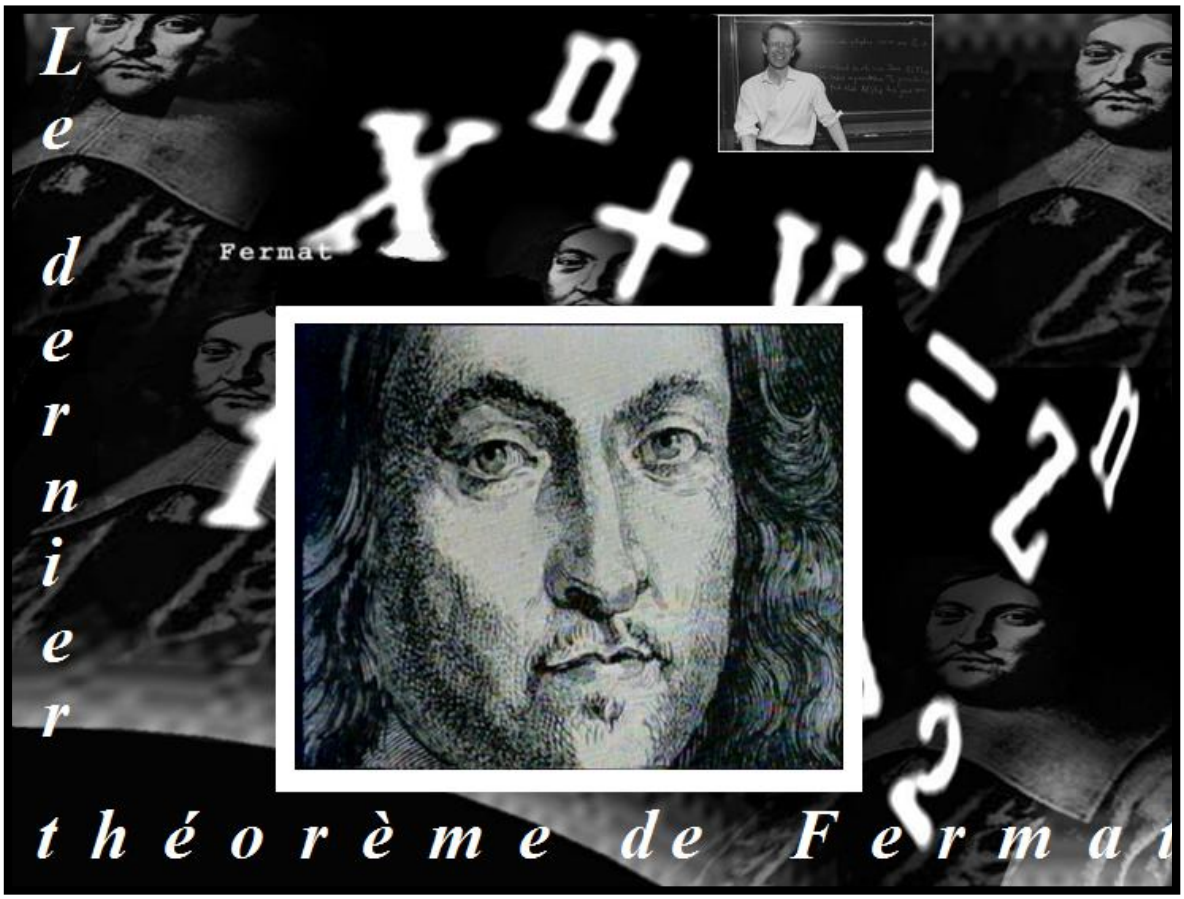
ACADEMIE
D'AIX-MARSEILLE

Activités autour du Dernier Théorème de Fermat



Document réalisé par Francis Loret
professeur agrégé de mathématiques
Irem, groupe vulgarisation

LE DERNIER THEOREME DE FERMAT

L'histoire du plus grand problème de maths de tous les temps

Plan des activités

Questionnaire préparatoire

EXPOSE CENTRAL

La boite à outil

Le raisonnement par contraposée

Le raisonnement par l'absurde

Le cas n= 2
équation $x^2 + y^2 = z^2$

La descente infinie

Le cas n= 4
équation $x^4 + y^4 = z^4$

Des résultats équivalents dans des domaines mathématiques différents

Équations diophantiennes

Courbes elliptiques et mathématiques de l'horloge

LE DERNIER THEOREME DE FERMAT

L'histoire du plus grand problème de maths de tous les temps

Questionnaire préparatoire

Questions scientifiques

1) Que signifient les écritures mathématiques suivantes :
7^2 ; 5^3 ; 2^4 ; x^n (où x est un nombre quelconque et n est un entier) ?

2) Combien de valeurs de x et de y peuvent vérifier l'égalité $x + y = 9$?
Donner des exemples.

3) Combien de valeurs de x, de y et de z peuvent vérifier l'égalité $x + y = 3z$?
Donner des exemples.

4) Vérifier que $x = 3$, $y = 4$ et $z = 5$ rend l'égalité $x^2 + y^2 = z^2$ vraie.
Y-a-t-il d'autres valeurs entières de x, de y et de z qui permettent de rendre vraie cette égalité ?
Donner des exemples.

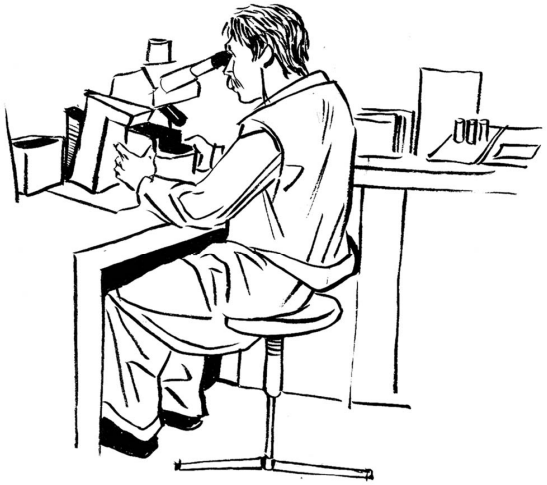
5) Comment illustrer facilement par la géométrie l'égalité $3^2 + 4^2 = 5^2$ en utilisant notamment un triangle ?

6) Est-il vrai que $6^3 + 8^3 = 9^3$? Seriez-vous capable de trouver des valeurs entières de x, de y et de z qui peuvent rendre vraie l'égalité $x^3 + y^3 = z^3$?

7) Qu'est-ce qu'une *conjecture* en mathématique ?

8) Qu'est-ce qu'un *nombre premier* ? Donner la liste de tous les nombres premiers inférieurs à 100.
Montrer que tous les nombres pairs supérieurs à 2 et inférieurs à 30 peuvent s'écrire comme la somme de deux nombres premiers.
Les nombres premiers de *Sophie Germain* sont des nombres premiers n tel que $2xn + 1$ soit aussi un nombre premier. Donner la liste des nombres premiers de *Sophie Germain* inférieurs à 100.

9) Qu'est-ce que *l'antimatière* en physique ? Qu'est-ce qu'un *trou noir* ?



Repères historiques et géographiques utiles

1) Placer sur la carte les villes d'Athènes, Alexandrie, Damas, Bagdad, Cordoue, Tolède, Palerme, Florence, Venise, Constantinople, Toulouse.

2) Sur quel support écrivait-on en Mésopotamie 2000 av. J.C. ?

3) Citer plusieurs grands mathématiciens de la Grèce antique.

4) Qui a fondé la ville d'Alexandrie d'Egypte ? En quelle année ?
Qu'est-ce que *la pierre de Rosette* ? Qu'a-t-elle permis ?
Qui était Diophante ? Quels livres importants a-t-il écrit ?

5) Quelle date marque la chute de l'Empire romain ?
Citer des exemples de peuples barbares qui déferlent sur l'Europe à partir de cette époque.

6) Jusqu'où s'étendent les conquêtes du monde musulman au VIII^{e} siècle ap. J.C. ?
Citer un grand mathématicien arabe à Bagdad au IX^{e} siècle ap. J.C.
Quel rôle jouent les *maisons de la Sagesse* dans le monde arabe à cette époque ?

7) Que s'est-il passé en 1453 ?
Que signifie le terme *Renaissance* en Italie au XV^{e} siècle ?

8) Qu'appelle-t-on le Grand Siècle ?

9) Qui était Marin Mersenne ? Qui était Pierre de Fermat ?

10) Qui était Sophie Germain ?

La boite à outil

Outil n°1 : trois nombres entiers x, y et z sont premiers entre eux dans leur ensemble signifie que le PGCD de ces trois nombres est 1.

Outil n°2 : si deux nombres entiers ne sont pas premiers entre eux, alors ils ont un diviseur commun d différent de 1.

Outil n°3 : si un nombre entier x est divisible par d, alors il peut s'écrire $x = d \times n$ où n est un nombre entier.

Outil n°4 : un nombre entier premier ne possède que deux diviseurs : lui-même et 1.

Outil n°5 : si x est un nombre entier pair, alors il peut s'écrire $x = 2p$ où p est un nombre entier.

Outil n°6 : si y est un nombre entier impair, alors il peut s'écrire $y = 2q + 1$ où q est un nombre entier.

Outil n°7 : si x et y sont des nombres entiers pairs, alors $x + y$ est également un nombre entier pair.

Outil n°8 : si x et y sont des nombres entiers impairs, alors $x + y$ est un nombre entier pair.

Outil n°9 : si x et y sont des nombres entiers de parité différente, alors $x + y$ est un nombre entier impair.

Outil n°10 : si x est un nombre entier pair, alors x^2 est un nombre entier pair.

Outil n°11 : si x est un nombre entier impair, alors x^2 est un nombre entier impair.

Outil n°12 : si le carré d'un nombre entier est pair, alors ce nombre entier est pair.

Outil n°13 : si le carré d'un nombre entier est impair, alors ce nombre entier est impair.

Outil n°14 : si d^2 divise x^2, alors d divise x.

Outil n°15 : u et v sont des nombres entiers premiers entre eux. Si le produit $u \times v$ est le carré d'un nombre entier, alors u et v sont chacun le carré d'un nombre entier.

Exercices

1. Pour tous : démontrer la validité des outils 7 à 11.
2. La validité des outils 10, 11, 12 et 13 sera démontrée dans une prochaine partie.
3. Pour les lycéens : démontrer la validité des outils 14 et 15.

LE DERNIER THEOREME DE FERMAT

L'histoire du plus grand problème de maths de tous les temps

Equations diophantiennes

Diophante était un mathématicien d'Alexandrie du III^{e} siècle après JC. Il est l'auteur de l'*Arithmétique*, livre qui aura une grande influence sur le travail des mathématiciens arabes, de la Renaissance et du Grand Siècle.

Pierre de Fermat avait pour livre de chevet un exemplaire de l'*Arithmétique* de Diophante, livre traduit en latin par son ami Claude-Gaspart Bachet de Méziriac. On trouve dans ce livre une somme de problèmes posés par le monde grec, notamment la résolution de certaines équations que l'on appelle *équations diophantiennes.* Ces équations ont la particularité de n'utiliser que des nombres entiers dans leur écriture, et de ne réclamer que des nombres entiers comme solution. En ce sens, l'équation du *Dernier Théorème de Fermat* est une équation diophantienne. Nous vous proposons dans cette activité d'étudier quelques solutions d'équations diophantiennes bien choisies, car la plupart sont très difficiles à résoudre.

1. Trouver un couple de nombres entiers x et y solution de l'équation : $x^3 - y^2 = 2$.

2. Trouver un couple de nombres entiers x et y solution de l'équation : $x^2 - 2y^2 = 1$.

3. Trouver un couple de nombres entiers x et y solution de l'équation : $x^2 - y^3 = 1$.

4. Trouver deux couples de nombres entiers x et y solutions de l'équation : $x^2 + 1 = 2y^4$.

Le premier couple de tête ? Le second à l'aide d'un tableur ?

5. Trouver un triplet de nombres entiers x, y et z solution de l'équation : $x^3 + y^3 = z^3 + 1$.

6. Trouver un quadruplet de nombres entiers x, y, z et t solution de l'équation : $x^3 + y^3 + z^3 = t^3$.

7. Il existe en fait une infinité de solutions entières à l'équation $x^3 + y^3 + z^3 = t^3$. Une formule mise au point par des mathématiciens consiste à choisir arbitrairement la valeur de deux entiers a et b et à remplacer ces deux nombres entiers dans chacune des quatre identités suivantes :

$$x = 28a^2 + 11ab - 3b^2 \qquad y = 21a^2 - 11ab - 4b^2$$
$$z = 35a^2 + 7ab + 6b^2 \qquad t = 42a^2 + 7ab + 5b^2$$

Etablir une liste de quelques solutions de cette équation (à la main, à la calculatrice où à l'aide d'un tableur).

De quoi s'agit-il ?

Andrew Wiles fait le vœu dès son plus jeune âge de résoudre le Dernier Théorème de Fermat. Il suivra ses études universitaires à Cambridge en Angleterre, la ville de sa naissance.

Un futur chercheur en mathématiques termine ses études par une thèse, c'est-à-dire qu'avec l'aide d'un professeur, il choisi d'explorer pendant trois ans un sujet que personne n'a encore approfondi.

Pour sa thèse, Andrew contacte John Coates, qui le dissuade de faire son sujet sur le Dernier Théorème de Fermat. Trop difficile, trop incertain. Il l'encourage à choisir son sujet dans le domaine des *courbes elliptiques*. Andrew accepte finalement la proposition de John, peut-être encouragé par le fait que Diophante avait consacré une bonne partie de son *arithmétique* aux courbes elliptiques et que Fermat en avait fait l'un de ses domaines d'étude. Andrew va devenir un spécialiste réputé de ces objets mathématiques difficiles. L'ironie du sort, c'est que ce sont ses compétences acquises sur les courbes elliptiques qui lui offriront le Dernier Théorème de Fermat…

Les courbes elliptiques portent mal leur nom puisque ce sont ni des courbes, ni des ellipses. Ce sont plutôt des équations, de la forme $y^2 + ay + b = x^3 + cx^2 + dx + e$ où a, b, c, d et e sont des nombres entiers. On leur a donné ce nom parce que dans le passé, elles servaient à mesurer le périmètre des ellipses et les longueurs des orbites des planètes.

Le défi avec les courbes elliptiques est de déterminer si elles ont des solutions en nombres entiers et si c'est le cas, de trouver le nombre de leurs solutions.

Un premier exemple

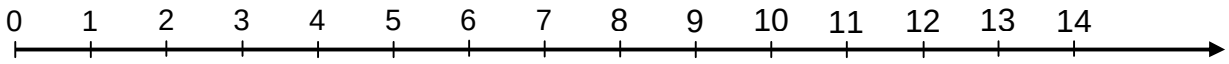
Fermat a prouvé que l'équation $y^2 = x^3 - 2$ qui est une courbe elliptique avec a = …, b = …, c = …
d = … et e = … n'a qu'un seul couple (x, y) solution avec x et y entiers naturels (compléter les pointillés). Trouver cette solution.

Les mathématiques de l'horloge

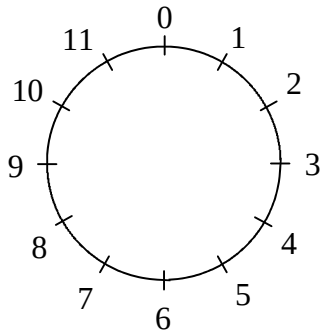
Dans les équations que Wiles étudie, il était si difficile de déterminer le nombre exact de solutions que la seule manière d'avancer un peu était de simplifier le problème. Par exemple, la courbe elliptique suivante : $y^2 + y = x^3 - x^2$ avec a = …, b = …, c = … d = … et e = … est presque impossible à attaquer directement (compléter les pointillés).
Le défi consiste à savoir combien de solutions en nombres entiers a cette équation.

1. Trouver deux couples de solutions (x, y) très simples de cette équation.

Il peut y avoir d'autres solutions, mais comme il y a une infinité de nombres entiers à explorer, il est très difficile d'établir la liste complète des solutions de cette équation. Il serait plus simple de chercher des solutions pour un ensemble fini de nombres, ce qui est possible dans ce que l'on appelle *les mathématiques de l'horloge*.
Les nombres entiers s'enchaînent à l'infini : 0, 1, puis 2, … et ces nombres peuvent être représentés comme des marques sur une ligne qui s'étend à l'infini.

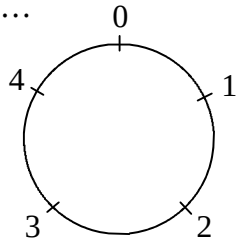


Sur cette ligne, nous nous représentons l'addition comme l'avancée à travers un certain nombre d'espaces. Par exemple, 4 + 2 = 6 équivaut à dire : commencez à 4, passez 2 espaces et arrivez à 6.
Par contre dans l'arithmétique de l'horloge, représentée cette fois sur un cercle, on retrouve le point de départ au bout d'un certain nombre :



- Dans une horloge classique qui contient 12 nombres du 0 au 11, 4 heures après 11 heures se dit 3 heures. C'est ce que l'on appelle en mathématique l'arithmétique du groupe cyclique à 12 éléments. Après le 11, il n'y a plus le 12, mais le zéro du départ.

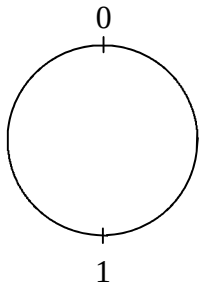
On peut imaginer aussi un groupe cyclique à 2 éléments, 3 éléments, 4 éléments,…



- Par exemple, dans une horloge qui contiendrait 5 nombres du 0 au 4, l'opération 3 + 2 donnerait 1 et l'opération 4 x 3 donnerait 2. Les tables d'additions et de multiplications dans les groupes cycliques deviennent alors très différentes de celles que l'on connaît habituellement.

2. Remplir les tables d'additions et de multiplications des groupes cycliques suivantes :

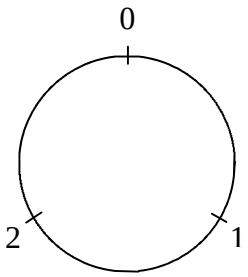
Groupe cyclique à 2 éléments



+	0	1
0		
1		

X	0	1
0		
1		

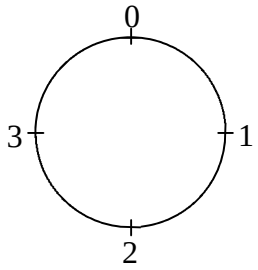
Groupe cyclique à 3 éléments



+	0	1	2
0			
1			
2			

X	0	1	2
0			
1			
2			

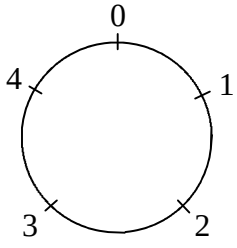
Groupe cyclique à 4 éléments



+	0	1	2	3
0				
1				
2				
3				

X	0	1	2	3
0				
1				
2				
3				

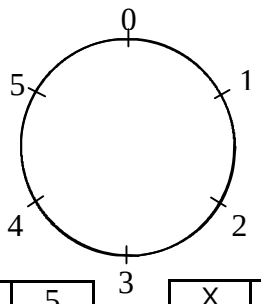
Groupe cyclique à 5 éléments



+	0	1	2	3	4
0					
1					
2					
3					
4					

X	0	1	2	3	4
0					
1					
2					
3					
4					

Groupe cyclique à 6 éléments



+	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

X	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

Etant donné que les groupes cycliques contiennent un nombre limité d'éléments, il est beaucoup plus facile d'établir toutes les solutions possibles d'une courbe elliptique pour chacun d'entre eux.

Par exemple, dans un groupe cyclique à 5 éléments, on peut établir toutes les solutions possibles de la courbe elliptique $y^2 + y = x^3 - x^2$.

Ce sont : $x = 0 \quad y = 0$ $\qquad$ $x = 1 \quad y = 0$

$x = 0 \quad y = 4$ $\qquad$ $x = 1 \quad y = 4$

Certaines de ces solutions, qui ne seraient pas valides en arithmétique classique, deviennent valides dans les groupes cycliques. Par exemple, la quatrième solution ($x = 1$ et $y = 4$) se vérifie ainsi :

$x^3 - x^2 = 1^3 - 1^2 = 1 - 1 = 0$

$y^2 + y = 4^2 + 4 = 1 + 4 = 0$ car dans ce groupe $4^2 = 1$ et $4 + 1 = 0$.

Liste L d'une courbe elliptique

Comme ils peinaient à faire l'inventaire de toutes les solutions des courbes elliptiques dans un espace infini, les mathématiciens cherchèrent le nombre de solutions dans chacun des groupes cycliques.

Par exemple, dans le groupe cyclique à 5 éléments, il y a 4 solutions, ce que l'on peut noter mathématiquement par : $L_5 = 4$. On peut alors établir la liste L_1, L_2, L_3,… d'une courbe elliptique qui représente un véritable trésor pour le spécialiste de la théorie des nombres. Elle contient une mine d'informations, une sorte de code génétique, qui sera utilisée par Wiles pour venir à bout de la conjecture de Taniyama/Shimura.

3. Etablir la liste L_1, L_2, L_3, L_4, L_5, … de la courbe elliptique $y^2 + y = x^3 - x^2$ (en essayant d'aller le plus loin possible).

Calcul de L_1 dans le groupe cyclique à 1 élément : ce groupe ne contient qu'un seul élément : 0

On calcule	$x^3 - x^2$
pour $x = 0$	

On calcule	$y^2 + y$
pour $y = 0$	

Conclusion : dans le groupe cyclique à 1 élément, il n'y a qu'une solution : (… ; ….).

D'où : $L_1 = \ldots$

Calcul de L_2 dans le groupe cyclique à 2 éléments : ce groupe contient les éléments : 0 ; 1

On calcule	$x^3 - x^2$
pour $x = 0$	
pour $x = 1$	

On calcule	$y^2 + y$
pour $y = 0$	
pour $y = 1$	

Conclusion : dans le groupe cyclique à 2 éléments, il y a … solutions : ……...

…… D'où : $L_2 = \ldots$

Calcul de L_3 dans le groupe cyclique à 3 éléments : ce groupe contient les éléments : ……..

On calcule	$x^3 - x^2$
pour $x = \ldots$	
pour $x = \ldots$	
pour $x = \ldots$	

On calcule	$y^2 + y$
pour $y = \ldots$	
pour $y = \ldots$	
pour $y = \ldots$	

Conclusion : dans le groupe cyclique à 3 éléments, il y a … solutions : ……...

…… D'où : $L_3 = \ldots$

Calcul de L_4 dans le groupe cyclique à 4 éléments : ce groupe contient les éléments : ……..

On calcule	$x^3 - x^2$
pour $x = \ldots$	
pour $x = \ldots$	
pour $x = \ldots$	
pour $x = \ldots$	

On calcule	$y^2 + y$
pour $y = \ldots$	
pour $y = \ldots$	
pour $y = \ldots$	
pour $y = \ldots$	

Conclusion : dans le groupe cyclique à 4 éléments, il y a … solutions : ……...

…… D'où : $L_4 = \ldots$

Calcul de L_5 dans le groupe cyclique à 5 éléments : ce groupe contient les éléments : ……..

On calcule	$x^3 - x^2$
pour x = …	
pour x = …	
pour x = …	
pour x = …	
pour x = …	

On calcule	$y^2 + y$
pour y = …	
pour y = …	
pour y = …	
pour y = …	
pour y = …	

Conclusion : dans le groupe cyclique à 5 éléments, il y a … solutions : ……...
…… D'où : L_5 = …

L_5 = …

Calcul de L_6 dans le groupe cyclique à 6 éléments : ce groupe contient les éléments : ……..

On calcule	$x^3 - x^2$
pour x = …	
pour x = …	
pour x = …	
pour x = …	
pour x = …	
pour x = …	

On calcule	$y^2 + y$
pour y = …	
pour y = …	
pour y = …	
pour y = …	
pour y = …	
pour y = …	

Conclusion : dans le groupe cyclique à 6 éléments, il y a … solutions : ……...
…… D'où : L_6 = …

Ce code génétique d'une courbe constitué par cette suite de nombre peut être comparé à une autre suite de nombres M_1, M_2, M_3, M_4, M_5, … véritable code génétique d'une forme modulaire. En 1955, Taniyama a remarqué une ressemblance : il prenait une forme modulaire et calculait le premier terme de la liste M et il remarquait que c'était le premier terme de la liste L d'une certaine courbe elliptique bien connue. Il continuait à calculer encore quelques termes de plus dans les 2 listes et constatait qu'il y avait toujours une parfaite égalité entre les nombres de ces listes. C'était une découverte étonnante, car avant Taniyama, personne ne soupçonnait une relation quelconque entre les courbes elliptiques et les formes modulaires. Pour les mathématiciens, ces objets étaient de nature très différente. Cette correspondance va jouer le rôle d'un véritable dictionnaire entre ces deux mondes, permettant de résoudre dans une théorie, des problèmes jusque là insolubles dans l'autre théorie.

Introduction

Une phrase comme :

si ABCD est un rectangle, alors ABCD a les diagonales de même longueur

est appelée en mathématique une **proposition**.

Cette proposition est vraie. Il existe bien sûr des propositions fausses.

On appelle **réciproque** de cette proposition la phrase que l'on obtient en échangeant la place de « ABCD est un rectangle » avec « ABCD a les diagonales de même longueur » :

si ABCD a les diagonales de même longueur, alors ABCD est un rectangle.

La réciproque d'une proposition est une nouvelle proposition et le fait que la proposition de départ soit vraie, ne signifie pas nécessairement que sa réciproque le sera. Dans notre exemple, la proposition est vraie et sa réciproque est fausse (si ABCD les diagonales de longueur et de même milieu, alors ABCD est un rectangle).

On appelle **contraposée de la proposition de départ** la phrase que l'on obtient d'une part en échangeant la place de « ABCD est un rectangle » avec « ABCD a les diagonales de même longueur », d'autre part en prenant leur **négation** :

*si ABCD **n'a pas** les diagonales de même longueur, alors ABCD **n'est pas** un rectangle.*

Les mathématiciens ont établis la preuve qu'une proposition et sa contraposée ont toujours la même valeur de vérité : si l'une est vraie alors l'autre l'est aussi et si l'une est fausse, l'autre l'est aussi.

Exemples

Compléter les tableaux suivants en indiquant dans la dernière colonne la valeur de vérité :

Proposition	*si ABCD est un carré, alors ABCD a 4 angles droits*	vraie
Réciproque		
Contraposée		

Proposition	*si AB = BC, alors B est le milieu de [AB]*	
Réciproque		
Contraposée		

Proposition	*si ABC est un triangle rectangle en A, alors* $BC^2 = AB^2 + AC^2$	
Réciproque		
Contraposée		

Application à l'arithmétique

1. Prouver de manière classique que *si x est un nombre entier naturel pair, alors* x^2 *est un nombre entier naturel pair.*
2. Prouver de manière classique que *si x est un nombre entier naturel impair, alors* x^2 *est un nombre entier naturel impair.*

Comme une proposition a la même valeur de vérité que sa contraposée, alors il peut être parfois judicieux, lorsqu'il est demandé de prouver une proposition, de chercher à prouver la contraposée.

3. Prouver en utilisant le principe de contraposée que *si le carré d'un nombre entier est pair, alors ce nombre entier est pair.*
4. Prouver de même en utilisant le principe de contraposée que *si le carré d'un nombre entier est impair, alors ce nombre entier est impair.*

LE DERNIER THEOREME DE FERMAT

L'histoire du plus grand problème de maths de tous les temps

Le raisonnement par l'absurde

En théorie des nombres, comme dans d'autres branches des mathématiques, on utilise un type de raisonnement qui s'avère dans certains cas très efficace : le raisonnement par l'absurde. La résolution par Wiles du *Dernier Théorème de Fermat* en est une nouvelle illustration.

De quoi s'agit-il ?

Pour prouver qu'une proposition est vraie, on va montrer que de supposer *le contraire* de la proposition à démontrer conduit à une absurdité mathématique, une incohérence logique. C'est notamment un principe très utilisé pour démontrer des propositions du type : « montrer que *ceci* .n'est pas… ». Etudions son fonctionnement sur un exemple :

Théorie	**Pratique**
Pour démontrer une proposition mathématique, …	$x = 0$ n'est pas une solution de l'équation $x + 1 = 0$
… on peut montrer que **de partir d'une hypothèse *contraire***…	…….. ……..
… **conduit**, par une suite de déductions, **à une** « **absurdité** »,…	…….. ……..
… c.à.d. que ce que l'on obtient dit le contraire de quelque chose de mathématiquement vrai.	Or, …….. …… est vraie.
Par conséquent :	…….. ……. est fausse.
Conclusion :	…….. …….. est vraie.

En résumé

1. On part de la négation de ce que l'on doit prouver et l'on teste les conséquences logiques de cette hypothèse.
2. Dès que l'on obtient une incohérence logique, on en déduit que cette supposition de départ est fausse.
3. Enfin, puisque la négation de la proposition est fausse, c'est que cette proposition est vraie.

Propositions à démontrer à l'aide de ce raisonnement

I. Prouver que les quotients $\frac{941664}{665857}$ et $\frac{665857}{470832}$ ne sont pas égaux :

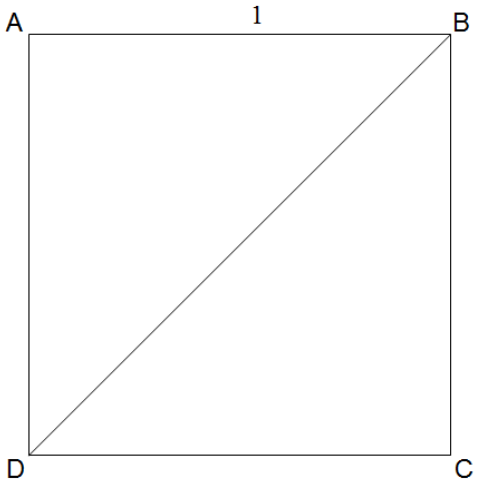
Théorie	**Pratique**
Pour démontrer une proposition mathématique, …	……..
… on peut montrer que **de partir d'une hypothèse *contraire***…	…….
… **conduit**, par une suite de déductions, **à une** « **absurdité** »,…	…….. ……..
… c.à.d. que ce que l'on obtient dit le contraire de quelque chose de mathématiquement vrai.	Or, …….. …… est vraie.
Par conséquent :	…….. …… est fausse.
Conclusion :	…….. …….. est vraie.

II. Le carré p^2 d'un nombre entier est pair. Prouver que ce nombre p est pair.

Théorie	Pratique
Pour démontrer une proposition mathématique, …	…….. ……..
… on peut montrer que **de partir d'une hypothèse *contraire***…	…….. ……..
… **conduit**, par une suite de déductions, **à une « absurdité »**,…	…….. ……..
… c.à.d. que ce que l'on obtient dit le contraire de quelque chose de mathématiquement vrai.	Or, …….. …… est vraie.
Par conséquent :	…….. ……. est fausse.
Conclusion :	…….. …….. est vraie.

III. Prouver de deux manières différentes que la diagonale d'un carré de côté 1 n'est pas exprimable sous la forme d'un quotient de deux nombres entiers.

A leur grande surprise, les mathématiciens grecs de l'Antiquité se sont rendus compte que la longueur de la diagonale d'un carré de côté 1 n'était pas « rationnelle », n'était pas exprimable sous forme de fraction.



On suppose que AC = $\frac{p}{q}$ où $\frac{p}{q}$ est une fraction non simplifiable (irréductible).

Méthode 1

1. Montrer que $AC^2 = 2$.
2. Montrer que $2q^2 = p^2$.
3. On va raisonner sur les chiffres des unités de p et de q. Remplir le tableau suivant :

Si le chiffre des unités de p est…	0	1	2	3	4	5	6	7	8	9
… alors le chiffre des unités de p^2 est…										

Si le chiffre des unités de q est…	0	1	2	3	4	5	6	7	8	9
… alors le chiffre des unités de q^2 est…										
… et le chiffre des unités de $2q^2$ est…										

4. En déduire que p devrait obligatoirement se terminer par … et que q devrait se terminer par … ou bien par ……
5. N'y a-t-il pas une contradiction avec la proposition de départ ?

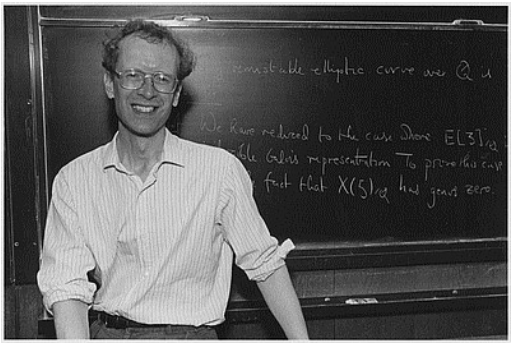
Méthode 2

1. Montrer que $AC^2 = 2$.
2. Montrer que $2q^2 = p^2$.
3. On va raisonner sur la parité de p et de q. Montrer que p est pair.
4. On peut donc écrire p sous la forme $p = 2k$ où k est un nombre entier. Montrer que q est pair.
5. N'y a-t-il pas une contradiction avec notre point de départ ?

IV. L'équation de Fermat $x^n + y^n = z^n$ n'a pas de solution non nulle pour tout entier *n* supérieur ou égal à 3.

Théorie	**Pratique**
Pour démontrer une proposition mathématique, …	L'équation de Fermat n'a pas de solution non nulle pour tout entier *n* supérieur ou égal à 3
… on peut montrer que **de partir d'une hypothèse *contraire***…	…….. ……..
… **conduit**, par une suite de déductions, **à une** « **absurdité** »,…	D'après ses calculs, en 1985 G. Frei pense que cette solution à l'équation de Fermat crée une …… ……. qui n'est pas …….. Ce sera prouvé plus tard par Ken Ribet.
… c.à.d. que ce que l'on obtient dit le contraire de quelque chose de mathématiquement vrai.	Or, Taniyama/Shimura exprime le fait que toute …… ……..……. est une ……... est vraie. Ce sera prouvé plus tard par Andrew Wiles.
Par conséquent :	…….. ……. est fausse.
Conclusion :	…….. …….. est vraie.





V. Les nombres premiers sont en nombre infini.

On suppose que les nombres premiers sont en nombre fini : $p_1, p_2, p_3, \ldots, p_n$ (il y en a n).
On introduit un nouveau nombre : $N = p_1 \times p_2 \times p_3 \times \ldots \times p_n + 1$

N est-il divisible par p_1,ou p_2, ou $p_3, \ldots$, ou p_n ?

Il y a alors 2 possibilités :

Soit N est un nouveau nombre premier. Montrer Alors que l'on obtient une contradiction.

Soit N n'est pas premier. Montrer alors que l'on peut trouver un nouveau nombre premier qui ne fait pas partie de la liste $p_1, p_2, p_3, \ldots, p_n$.. Montrer alors que l'on obtient une contradiction.

LE DERNIER THEOREME DE FERMAT

L'histoire du plus grand problème de maths de tous les temps

Le cas n = 2

De quoi s'agit-il ?

Dans l'Antiquité, les Babyloniens avaient trouvé quelques triplets de nombres entiers qui vérifiaient l'équation $x^2 + y^2 = z^2$. Par la suite, les Grecs montrèrent que l'on peut trouver une infinité de triplets de nombres entiers solutions de cette équation. Ils montrèrent même les formules permettant de les trouver tous. Cette activité propose de retrouver ces formules…

Comment déterminer tous les triplets (x, y, z) d'entiers naturels vérifiant l'équation $x^2 + y^2 = z^2$?

PARTIE I

Supposons que le triplet d'entier (x', y', z') soit une solution de cette équation.

1. Comment choisir l'entier d et trois entiers x, y, z tels que $x' = d \times x$, $y' = d \times y$, $z' = d \times z$ tels que x, y, z soient premiers entre eux dans leur ensemble ?

2. Prouver alors que (x, y, z) est aussi solution de cette équation.

3. Prouver par un raisonnement par l'absurde que les entiers x, y, z sont premiers entre eux deux à deux.

4. En déduire que x, y ne peuvent pas être tous les deux pairs.

5. Prouver par un raisonnement par l'absurde que x, y ne peuvent pas être tous les deux impairs :
   - écrire x et y sous la forme $2p + 1$ et $2q + 1$.
   - Prouver que la somme de leur carré vaut $2 \times [2(p^2 + q^2 + p + q) + 1]$.
   - En déduire que z est pair.
   - Ecrire z sous la forme $2r$.
   - Montrer alors que l'égalité $x^2 + y^2 = z^2$ devient $2 (p^2 + q^2 + p + q) + 1 = 2r^2$.
   - Conclusion.

6. Montrer que z est impair.

Bilan de la partie I

Les entiers x, y, z sont premiers entre eux deux à deux.

Si x est pair, alors est y est impair (et réciproquement).

z est impair.

PARTIE II

Supposons alors que x soit le nombre entier pair et que y soit le nombre entier impair.

7. Montrer que $z - y$ et $z + y$ sont pairs.

8. On pose alors $z + y = 2u$ et $z - y = 2v$. Montrer que $y = u - v$ et que $z = u + v$.

9. Prouver par un raisonnement par l'absurde que les entiers u et v sont premiers entre eux.

10. Montrer que $x^2 = 4\ u \times v$.

11. En déduire que u et v sont chacun le carré d'un nombre entier.

12. On pose alors $u = a^2$ et $v = b^2$. Prouver par un raisonnement par l'absurde que les nombres entiers a et b sont premiers entre eux.

PARTIE III : conclusion

13. Prouver que les formules donnant les triplets (x', y', z') solutions de cette équation sont :

$x' = 2\ d \times a \times b$ $\qquad$ $y' = d \times (a^2 - b^2)$ $\qquad$ $z' = d \times (a^2 + b^2)$

14. Vérifier que ces valeurs sont effectivement solutions de l'équation : $x^2 + y^2 = z^2$.

15. Calculer une liste d'exemples de triplets de nombres entiers (premiers dans leur ensemble) vérifiant cette équation :

a	b	x	y	z	$x^2 + y^2$	z^2

Cette méthode apparaît dans les Éléments d'Euclide, mais c'est surtout Fermat qui la formule explicitement et en fait un instrument important dans son programme pour la théorie des nombres entiers. Elle sera notamment utilisée pour prouver le cas $n = 4$.

De quoi s'agit-il ?

Cette méthode sert essentiellement à démontrer qu'il **n'existe pas** de nombres entiers naturels répondant à une certaine propriété.

On suppose au départ que ces entiers naturels qui répondent à la propriété existent.

On construit alors une nouvelle solution valable pour un entier naturel strictement plus petit que l'entier naturel précédent. Rien n'empêche alors de construire une nouvelle solution plus petite, puis encore une nouvelle… et de reproduire ce mécanisme à l'infini. Oui, mais… il est impossible de rendre indéfiniment plus petits les termes d'une suite de nombres entiers naturels ! On arrive donc à une absurdité… ce qui contredit la supposition de départ.

A démontrer par une descente infinie…

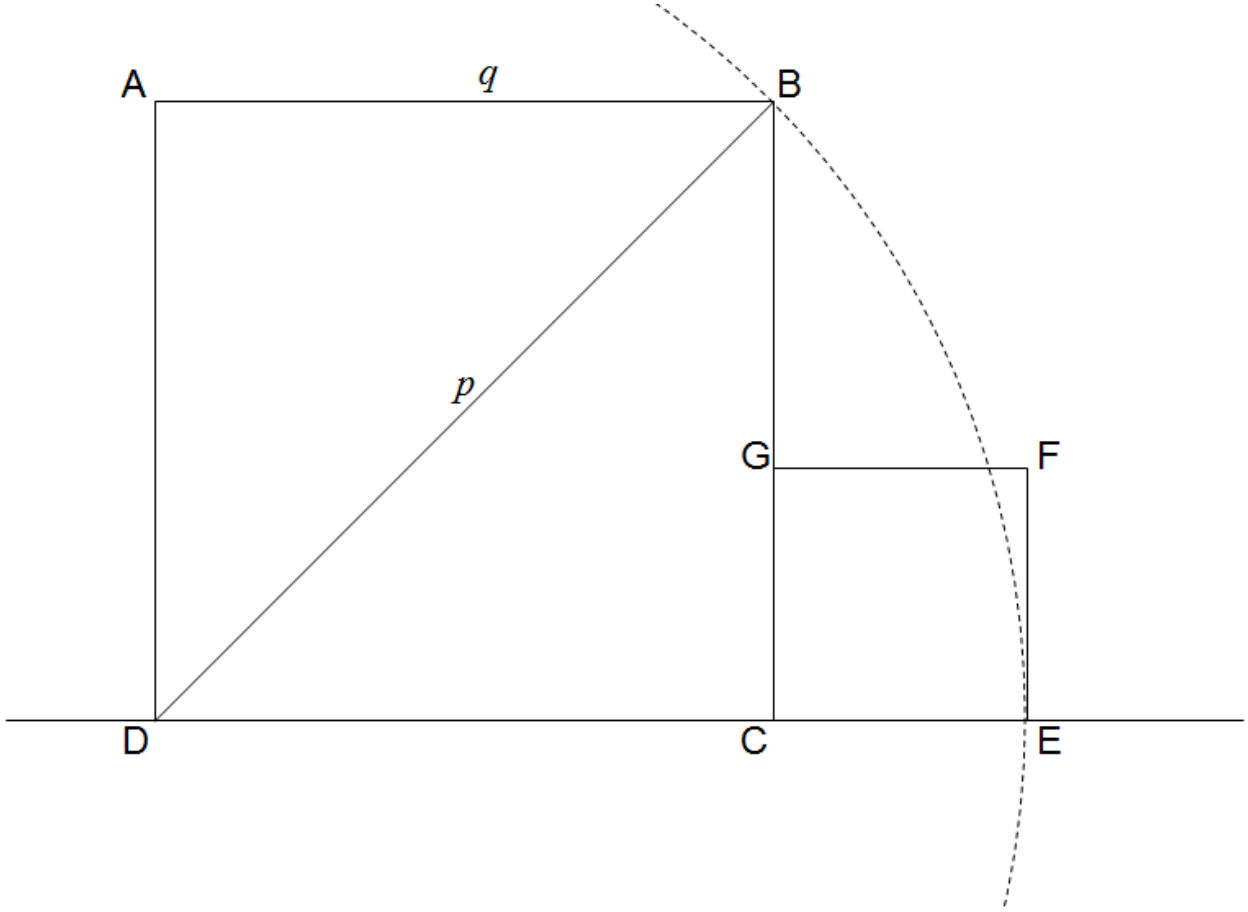
I. Montrer qu'il n'existe pas de nombres entiers naturels non nuls x et y tels que $x^2 = 2y^2$.

Supposons qu'il existe de tels entiers.

1. Montrer que x est pair. On pose $x = 2x_1$.
2. Montrer que $x_1^2 = 2y_1^2$
3. Combien de fois peut-on reproduire cette opération ?
4. Conclure.

II. Prouver que la diagonale d'un carré n'est pas exprimable sous la forme d'un quotient de deux entiers.

A partir du carré ABCD, on construit le carré CEFG comme indiqué ci-dessus : on reporte la longueur DB sur la droite (CD).



Supposons que le rapport de BD et AB soit une fraction p/q avec p et q entiers naturels non nuls. On peut alors choisir l'unité du dessin pour que DB = p et AB = q.

1. Prouver que CE est encore un nombre entier, inférieur à q.
2. Prouver que $p^2 = 2q^2$.
3. Le carré CEFG est une réduction du carré ABCD. Prouver que l'échelle de réduction vaut $p/q - 1$?
4. Prouver que CF est encore un nombre entier, inférieur à p.
5. Combien de fois peut-on reproduire cette construction géométrique ?
6. N'y aura-t-il pas numériquement un problème ?
7. Conclure.

Le cas $n = 4$ est certainement le premier cas à avoir été démontré. Il est fort probable que Fermat en avait réellement trouvé la preuve. Il s'appuie sur une descente infinie et également sur la connaissance du cas $n = 2$.

Bilan du cas n = 2

Que peut-on dire des triplets (x, y, z) d'entiers vérifiant l'équation $x^2 + y^2 = z^2$?

Ces triplets sont appelés triplets Pythagoriciens. Les triplets (x, y, z) premiers entre eux dans leur ensemble sont appelés les triplets Pythagoriciens primitifs. Dans ce cas :

- **Les entiers x, y, z sont premiers entre eux deux à deux.**
- **Si x est pair, alors y est impair (et réciproquement).**
- **z est impair.**
- **$x = 2ab$ $y = a^2 - b^2$ $z = a^2 + b^2$ où a et b sont des entiers premiers entre eux (avec $a > b$).**

Le cas n = 4

PARTIE I

On s'intéresse à l'équation $x^4 + y^4 = z^2$

Démontrer que si l'on prouve que l'équation $x^4 + y^4 = z^2$ n'a pas de solutions en nombres entiers différents de zéro, alors on aura prouvé que l'équation $x^4 + y^4 = z^4$ n'a pas de solutions en nombres entiers différents de zéro.

PARTIE II

Supposons que le triplet d'entiers (x, y, z) soit une solution de l'équation $x^4 + y^4 = z^2$

1. d est le PGCD de x et y. Montrer d^2 divise z.

Quitte à simplifier cette équation par d^4, on peut alors supposer comme dans le cas $n = 2$ que x , y et z sont premiers entre eux dans leur ensemble. Le triplet (x^2, y^2, z) est donc pythagoricien primitif.

On peut donc écrire : $x^2 = 2ab$, y^2 = ……. *et* z = …….. où a et b sont des nombres entiers ……..……..……

On va à présent construire une descente infinie :

2. Prouver que le triplet (b, y, a) est encore un triplet Pythagoricien primitif.

On peut donc écrire : $b = 2mn$, y =…….. *et* a = …….. où m et n sont des nombres entiers ……..……..……

3. Prouver que les entiers a, m et n sont tous les trois des carrés.

4. On peut alors écrire : $a = z'^2$ $m = x'^2$ $n = y'^2$ où x', y'et z' sont des nombres entiers.

Prouver que le triplet d'entier (x', y', z') est encore solution de l'équation $x^4 + y^4 = z^2$.

5. Prouver que $0 < z' < z$.

6. Conclure.

De quoi s'agit-il ?

La plupart des personnes pensent que les mathématiques, ce n'est qu'une seule matière. Pourquoi ne pas dire alors que nous faisons de *la mathématique* ? Pourquoi mettre au pluriel ? Parce que les mathématiques sont constituées de nombreuses disciplines, parfois très différentes les unes des autres.
Au collège, on débute l'étude de l'arithmétique, l'algèbre, la géométrie, des statistiques… Au lycée, on rajoute l'analyse, les probabilités, … et dans le supérieur, le nombre des domaines d'étude devient encore plus grand. Chacun de ces domaines a ses propres systèmes de signes, son propre langage, parfois incompréhensible pour les mathématiciens des autres domaines.
Le rêve de certains mathématiciens, comme par exemple Robert Langlands, est de construire des passerelles entre ces différents domaines.
A l'image de la Pierre de Rosette qui a permis de faire le lien entre le démotique égyptien, le grec et les hiéroglyphes, ces ponts pourraient permettre d'obtenir un véritable dictionnaire pour traduire des problèmes non résolus d'un langage à un autre, en cherchant celui qui serait le plus adapté.
La preuve du Dernier Théorème de Fermat est remarquable sur ce point : Wiles prouve la conjecture de Taniyama/Shimura qui établit un véritable dictionnaire pour traduire les problèmes exprimés dans le langage des courbes elliptiques, en problèmes exprimés dans le langage des formes modulaires, deux domaines apparemment très éloignés.
Plus proche de nous, il peut être très intéressant de chercher à traduire des problèmes de *nombres* en problèmes de *formes* (et inversement), en utilisant le pont qui existe entre la théorie des nombres et la géométrie.

Traduire des problèmes de nombres en problèmes de formes

I. Illustrer par des constructions géométriques les égalités :

$k \times (a + b) = k \times a + k \times b$

$(a + b)^2 = a^2 + 2ab + b^2$

$3^2 + 4^2 = 5^2$

II. Traduction dans le langage de la géométrie de l'énoncé *$x^4 + y^4 = z^2$ n'a pas de solutions en nombres entiers non nuls.*

On va montrer que l'énoncé A :

l'équation $x^4 + y^4 = z^2$ n'a pas de solutions en nombres entiers non nuls

en arithmétique est équivalent en géométrie à l'énoncé B :

il n'existe pas de rectangle dont les côtés et la diagonale sont des entiers (différents de zéro) ayant la même aire qu'un carré dont le côté est un entier.

Pour montrer que ces deux propositions mathématiques sont équivalentes,

- on va prouver d'abord que A implique B (implication) ;
- on va prouver ensuite que B implique A (réciproque).

On va prouver d'abord par contraposée que

si l'équation $x^4 + y^4 = z^2$ n'a pas de solutions en nombres entiers non nuls,

alors

il n'existe pas de rectangle dont les côtés et la diagonale sont des entiers (différents de zéro) ayant la même aire qu'un carré dont le côté est un entier.

1. S'il existe un rectangle dont les côtés *a* et *b* et la diagonale *c* sont des nombres entiers (différents de zéro) ayant la même aire qu'un carré dont le côté est un nombre entier, alors montrer que *a* et *b* peuvent s'écrire sous forme de carrés (quitte à simplifier *a* et *b* par leur PGCD, on peut alors supposer que *a* et *b* sont premiers entre eux).
2. Montrer alors qu'il existe une solution en nombres entiers non nuls à l'équation $x^4 + y^4 = z^2$.
3. Conclure.

On va prouver ensuite par contraposée que

s'il n'existe pas de rectangle dont les côtés et la diagonale sont des entiers (différents de zéro) ayant la même aire qu'un carré dont le côté est un entier,

alors

l'équation $x^4 + y^4 = z^2$ n'a pas de solutions en nombres entiers non nuls.

1. S'il existe une solution en nombres entiers non nuls (x, y, z) à l'équation $x^4 + y^4 = z^2$, montrer alors que l'on peut trouver un rectangle dont les côtés et la diagonale sont des entiers (différents de zéro) ayant la même aire qu'un carré dont le côté est un entier.
2. Conclure.