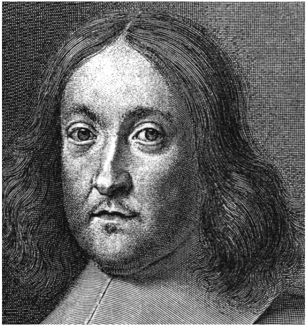
Le fabuleux destin du théorème de Fermat

A.-M. Aebischer

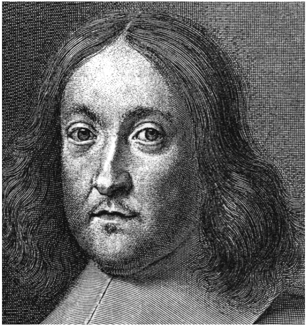
IREM de Franche-Comté

Pierre de Fermat



Pierre de Fermat
(1605 ?-1665)
Conseiller
au parlement de Toulouse

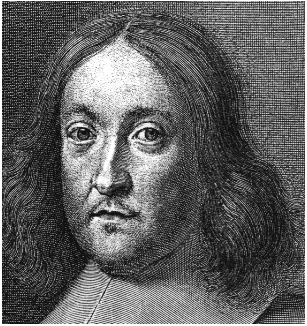
Pierre de Fermat



« J'ay si peu de commodité d'escrire mes démonstrations, que je me contente d'avoir découvert la vérité et de sçavoir le moyen de la prouver, lorsque j'auray le loisir de le faire. »

« Je ne doute pas que la chose n'eût pu se polir davantage, mais je suis le plus paresseux de tous les hommes. »

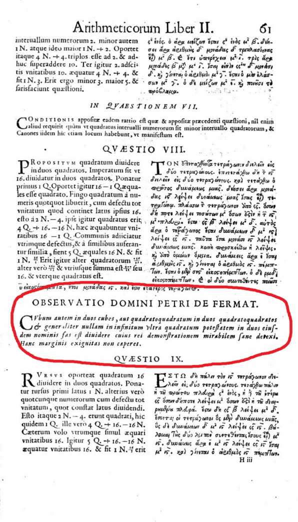
Pierre de Fermat



« J'ay si peu de commodité d'escrire mes démonstrations, que je me contente d'avoir découvert la vérité et de sçavoir le moyen de la prouver, lorsque j'auray le loisir de le faire. »

« Je ne doute pas que la chose n'eût pu se polir davantage, mais je suis le plus paresseux de tous les hommes. »

Une énigme vieille de 350 ans



Arithmeticorum Liber II. 61

interuallum numerorum 2. minor autem 1 N. atque ideo maior 1 N. + 2. Oportet itaque 4 N. + 4. triplos esse ad 2. & adhuc superaddere 10. Ter igitur 2. adscitis vnitatibus 10. æquatur 4 N. + 4. & fit 1 N. 3. Erit ergo minor 3. maior 5. & satisfaciunt quæstioni.

IN QVAESTIONEM VII.

CONDITIONIS appositæ eadem rattio est quæ & appositæ præcedenti quæstioni, nil enim aliud requirit quàm vt quadratus interualli numerorum sit minor interuallo quadratorum, & Canones iidem hic etiam locum habebunt, vt manifestum est.

QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum sit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 − 1 Q. æquales esse quadrato. Fingo quadratum à numeris quotquot libuerit, cum defectu tot vnitatum quod continet latus ipsius 16. esto à 2 N. − 4. ipse igitur quadratus erit 4 Q. + 16. − 16 N. hæc æquabuntur vnitatibus 16 − 1 Q. Communis adiiciatur vtrimque defectus, & à similibus auferantur similia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{16}{5}$ Erit igitur alter quadratorum $\frac{256}{25}$. alter verò $\frac{144}{25}$ & vtriusque summa est $\frac{400}{25}$ seu 16. & vterque quadratus est.

OBSERVATIO DOMINI PETRI DE FERMAT.

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

QVÆSTIO IX.

RVRSVS oporteat quadratum 16 diuidere in duos quadratos. Ponatur rursus primi latus 1 N. alterius verò quotcunque numerorum cum defectu tot vnitatum, quot constat latus diuidendi. Esto itaque 2 N. − 4. erunt quadrati, hic quidem 1 Q. ille verò 4 Q. + 16. − 16 N. Cæterum volo vtrumque simul æquari vnitatibus 16. Igitur 5 Q. + 16. − 16 N. æquatur vnitatibus 16. & fit 1 N. $\frac{16}{5}$ erit

H iii

On ne peut exprimer un cube comme une somme de deux cubes, un bicarré comme une somme de deux bicarrés, et plus généralement une puissance parfaite comme une somme de deux mêmes puissances.

J'en ai découvert une démonstration tout à fait remarquable. Mais ma marge est trop étroite pour la contenir.

L'énigme

Autrement dit :

L'équation

$$x^n + y^n = z^n$$

n'a pas de solutions entières (non triviales) pour $n \geqslant 3$.

Cette affirmation est le *dernier théorème de Fermat*.

ne fut résolue qu'en 1995 !

Passioné depuis l'enfance par le théorème de Fermat ...

Andrew Wiles
23 Juin 1993
Cambridge

je crois que je m'arrêterai là !

Le cas $n = 2$

Les mathématiciens de l'antiquité (Pythagore, Platon, Euclide) ont complétement résolu l'équation (en nombres entiers)

$$x^2 + y^2 = z^2$$

Les solutions sont les entiers (x, y, z) de la forme

$$(x = 2nm, y = n^2 - m^2, z = n^2 + m^2) \quad \text{avec } n \text{ et } m \text{ entiers}$$

.

Exemple : $n = 2, m = 1$, alors $x = 4$, $y = 3$ et $z = 5$.

Une démonstration de Fermat pour $n = 4$

Sa méthode est restée célèbre sous le nom de *descente infinie de Fermat*.

La descente infinie

Fermat a plutôt étudié l'équation

$$X^4 + Y^4 = Z^2$$

Si (x, y, z) vérifie $x^4 + y^4 = z^4$, alors (x, y, z^2) vérifie

$$X^4 + Y^4 = Z^2$$

Donc, si l'équation $X^4 + Y^4 = Z^2$ n'a pas de solutions entières, l'équation $x^4 + y^4 = z^4$ non plus !

La descente infinie

Fermat a alors montré que s'il existe une solution (x, y, z) à l'équation $X^4 + Y^4 = Z^2$, il pouvait en fabriquer une autre $(x', y,' z')$ avec $z' < z$.

Or, il est impossible de descendre infiniment dans les entiers naturels...

	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

Fermat a prouvé le cas $n = 4$.

Soit (a, b, c) vérifiant : $a^8 + b^8 = c^8$

ou encore $$(a^2)^4 + (b^2)^4 = (c^2)^4$$

Alors (a^2, b^2, c^2) est solution de $X^4 + Y^4 = Z^4$. IMPOSSIBLE !

Donc l'équation $x^8 + y^8 = z^8$ n'a pas de solution.

	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

On peut éliminer de la liste des entiers les multiples de 4.

	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

(1753) Euler démontre le cas $n = 3$.

	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

On peut éliminer de la liste des entiers les multiples de 3.

Il suffit de démontrer le théorème de Fermat pour des exposants premiers.

Sophie Germain

- Sophie Germain (1776 - 1831) ;
- mathématicienne et physicienne de talent ;
- elle élabore une méthode pour prouver le théorème de Fermat dans un grand nombre de cas (1825).

Elle crée une avancée significative dans la recherche autour du théorème.

Bref...

En 1857 :

- le théorème a été vérifié pour presque tous les entiers inférieurs à 100 ;
- certains entiers font de la résistance ;
- il n'y a plus de progrès significatifs ;
- le théorème de Fermat tombe progressivement dans l'oubli.

En 1908, Paul Wolfskehl institue une récompense de **100 000 marks** pour la démonstration du théorème de Fermat.

Cher. . .. . .

Vous nous avez soumis une démonstration du théorème de Fermat.

La première erreur se trouve :

Page : . . .. . .   Ligne :. . .. . .

Ceci invalide votre démonstration.

Bien cordialement,

Pr. E. Landau

J'ai trouvé une erreur dans votre démonstration.
Cette page est trop étroite pour contenir tous les détails de la réfutation.

Je ne suis pas qualifié pour analyser votre preuve.
Voici l'adresse d'un expert qui pourra l'analyser :

(adresse de l'auteur de la précédente proposition de démonstration fausse)

Des objets mathématiques nouveaux

- les courbes elliptiques (E) ;
- les formes modulaires (M).

Chaque objet existe dans un domaine bien spécifique de la

théorie des nombres

Sans rapport ?

Chacun peut être caractérisé par une série de nombres : "son ADN".

(E) $(E_1, E_2, \ldots, E_n, \ldots)$

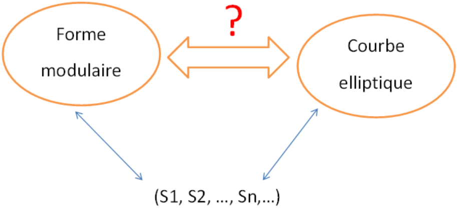
(M) $(M_1, M_2, \ldots, M_n, \ldots)$

Acte 1 : Tanyama/ Shimura

Tanyama

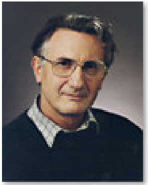
Shimura

Colloque Tokyo (1955)



Conjecture de Tanyama/Shimura/Weil

Acte 2 : 1984



Y. Hellegouarch

G. Frey

Hellegouarch (Thèse à Besançon !) puis G. Frey ont l'idée d'associer une courbe elliptique à une hypothétique solution du théorème de Fermat.

→ **Il semble que cette courbe ne soit pas modulaire !**

Acte 3 : 1986

K. Ribet

1986 : Ken Ribet démontre la conjecture de Frey....

S'il existe une solution à l'équation de Fermat, la courbe elliptique qui lui est associée n'est pas modulaire.

Bref...

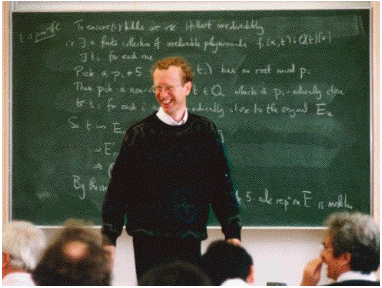
Théorème de Fermat		Conjecture T.S.W.
FAUX	$\Rightarrow$	**FAUSSE**
(existence d'une solution)		(une certaine courbe elliptique n'est pas modulaire)

Ou alors ...

Théorème de Fermat		Conjecture T.S.W.
VRAI	$\Leftarrow$	**VRAIE**
(pas de solution)		(toute courbe elliptique est modulaire)

Acte 4 : Andrew Wiles

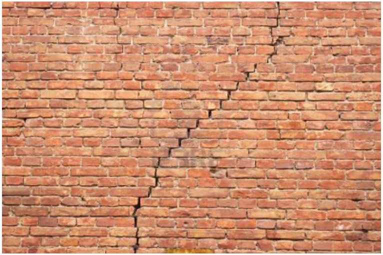
Acte 4 : Andrew Wiles



Andrew Wiles
23 Juin 1993
Cambridge

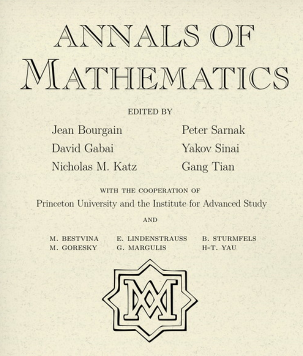
je crois que je m'arrêterai là...

Acte 4 : Andrew Wiles



Octobre 1993 : une faille dans la démonstration ?

Acte 4 : Andrew Wiles



1995
résultat validé et publié !

Annals of Mathematics, **142** (1995), 443–551

Modular elliptic curves and Fermat's Last Theorem

By Andrew Wiles*

For Nada, Clare, Kate and Olivia

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

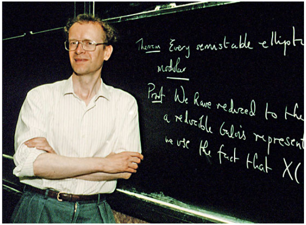
Pierre de Fermat

Introduction

An elliptic curve over **Q** is said to be modular if it has a finite covering by a modular curve of the form $X_0(N)$. Any such elliptic curve has the property that its Hasse-Weil zeta function has an analytic continuation and satisfies a functional equation of the standard type. If an elliptic curve over **Q** with a given j-invariant is modular then it is easy to see that all elliptic curves with the same j-invariant are modular (in which case we say that the j-invariant is modular). A well-known conjecture which grew out of the work of Shimura and Taniyama in the 1950's and 1960's asserts that every elliptic curve over **Q** is modular. However, it only became widely known through its publication in a paper of Weil in 1967 [We] (as an exercise for the interested reader!), in which, moreover, Weil gave conceptual evidence for the conjecture. Although it had been numerically verified in many cases, prior to the results described in this paper it had only been known that finitely many j-invariants were modular.

In 1985 Frey made the remarkable observation that this conjecture should imply Fermat's Last Theorem. The precise mechanism relating the two was formulated by Serre as the ε-conjecture and this was then proved by Ribet in the summer of 1986. Ribet's result only requires one to prove the conjecture for semistable elliptic curves in order to deduce Fermat's Last Theorem.

*The work on this paper was supported by an NSF grant.



Merci de votre attention !