



Grupo PET Computação
DSC – CEEI



**Ciclo de
Seminários**

O Último Teorema de Fermat

Um enigma de 358 anos

Carlos Rafael Rego da Silva
carlos.rafael.silva@ccc.ufcg.edu.br

Agenda

- Pierre de Fermat
- Último Teorema
- Leonard Euler
- Sophie Germain
- Evaristè Galois
- Paul Wolfskehl
- Cultura Pop
- Testes computacionais
- Andrew Wiles

“Você sabe”, admitiu o Diabo, “nem mesmo os melhores matemáticos de outros planetas, todos muito mais avançados que o seu, conseguiram resolvê-lo. Tem um sujeito em Saturno, ele parece com um cogumelo sobre pernas de pau, que resolve mentalmente equações diferenciais parciais, e mesmo ele desistiu.

— Arthur Poges em “O diabo e Simon Flagg”(1954)

uktv
DOCUMENTARY

UKTV Guide ●

Pierre de Fermat

mathematicus nascitur, non fit

- 20 de agosto de 1601, Sudoeste da França
- Monastério de Grandselve
- Serviço público
- “Morte” em 1652
- Matemática – “hobby”
- “Príncipe dos Amadores”
- “Fanfarrão” – René Descartes
- “Aquele maldito francês” – John Wallis



Pierre de Fermat

- Teoria da Probabilidade
- Teoria dos Números
- Frequentemente, criava cartas enunciando seu mais recente teorema, como forma de desafio a outros matemáticos, sem fornecer a demonstração.



Ultimo Teorema

- O livro *Aritimetica* de Diofante continha mais de 100 problemas, os quais Fermat explorou por vários anos.
- *Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.*

intervallum numerorum 2. minor autem
1 N. atque ideo maior 1 N. + 2. Oportet
itaque 4 N. + 4. triplos esse ad 2. & ad-
huc superaddere 10. Ter igitur 2. adscis-
tis vnitibus 10. æquatur 4 N. + 4. &
fit 1 N. 3. Erit ergo minor 3. maior 5. &
satisfaciunt quæstioni.

ϵ^{α} ἰός. οὐ ἀρε μείζον ἔτσι ϵ^{β} ἰός μ^{β} . δ' ἴ-
σει ἀρε ἀρβυλῶν δ' μονάδους δ' τριπλασιάζας
 η^{γ} μ^{β} . εἰ ἔτι υπερίχεται μ^{δ} . τὰς ἀρε
μονάδας β' μ^{γ} μ^{δ} . ὅση εἴη ϵ^{α} δ' μονά-
δ'. καὶ γήταται οὐ ἀρβυλῶν μ^{γ} . ἔτσι οὐ μὲν ἐλά-
σαι μ^{δ} . οὐ δὲ μείζον μ^{ϵ} . καὶ πυνύει τὸ
ποσὸν μ^{ζ} .

IN QVAESTIONEM VII.

CONDITIONES appositæ eadem ratio est quæ & appositæ præcedenti quæſtioni, nil enim aliud requirit, quàm ut quadratus intervalli numerorum ſit minor intervallo quadratorum, & Canones iidem hic etiam locum habebunt, ut manifeſtum eſt.

QVÆSTIO VIII.

PROPOSITUM quadratum diuidere in duos quadratos. Imperatum fit vt 16. diuidatur in duos quadratos. Ponatur primus 1. Q. Oportet igitur 16-1. Q. æquales esse quadratos. Fingo quadratum à numero quotquot libuerit, cum defectu totum vnitum quod continet latus ipsius 16. effo à N. -4. ipse igitur quadratus erit 4 Q. + 16. -16. N. hæc æquabuntur vnitatibus 16. -1. Q. Communis adiciatur vtriusque defectus, & à similibus auferatur totum familia, sient 5. Q. æquales 16. N. & fit 1. N. ¹ Erigit igitur alter quadratorum 16. alter vero 5. & vtriusque summa est 21. seu 16. & vterque quadratus est.

ΤΟΝ ὑποταχέναν τετραρχίαν· διελόν εἰς
 δύο τετραρχίας. ὑποταχέναν δὲ τὴν
 διάνειαν τῶν τετραρχούντων καὶ τιτάντων
 ἀποφθόνου διωκόμενος μακάρι, δίδωσι ἀπὸν μακάρι-
 ον καὶ λαλοῦν διδασκόμενος μακάρι Ἰσάκ (ἢ) τὴν
 τετραρχίαν. πάλαιον δὲ τετραρχούντων δύο καὶ ὅσον
 δὲ ποτα λείπει ποσόντων μὴ ὅσον ὅστις τὴν
 μὴ πάλαιον. ἰσὺν εἰς β' λαλοῦν δὲ αὐτὸς
 ἀπὸν τὴν τετραρχίαν ἔχει διδασκόμενος δὲ μὴ καὶ
 λαλοῦν εἰς τὴν. πάλαιον τὴν ποσότητα καὶ λαλοῦν
 διδασκόμενος ποσὴν ποσότητα καὶ λαλοῦν
 καὶ ποσὴν ὁμοίαν ὁμοίαν. διδασκόμενος ἀπὸν τὴν
 ἀπομνησμένην καὶ ὁμοίαν ἀπομνησμένην. ἰσὺν
 ποσότητα. ἰσὺν δὲ αὐτὸν ἑξαιρούμενον. δὲ ἰσὺν
 ἑξαιρούμενον. ἑὶ οὐ δύο σωτηριότητις ποσὴν
 ἰσὺν ποσότητα.

OBSERVATIO DOMINI PETRI DE FERMAT.

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

QVÆSTIO IX.

R VRSVS oporteat quadratum 16
dividere in duos quadratos. Ponatur
rursus primi lateris 1 N. alterius vero
quocunque numerorum cum defectu tot
vnitatum, quot constet lateris diuidenti.
Elo itaque 2 N. - 4. erunt quadrati, hic
quidam 1 Q. ille vero 4 Q. + 16. - 16 N.
Caterum volo vtrumque simul æquari
vnitatribus 16. Igitur 5 Q. + 16. - 16 N.
æquatur vnitatribus 16. & fit 1 N. 7 erit

[illegible]

uktv
DOCUMENTARY

$$x^2 +$$

Leonard Euler

- Provou alguns teoremas de Fermat:
 - Todos primos da forma $4n-1$ são somas de dois quadrados. ($13 = 2^2 + 3^2$)
- Desenvolve diversos algoritmos, inclusive para a previsão das fases da Lua.
- Ponte de Königsberg.
- Provou que não existem soluções para $n=4$ e $n=3$ (surgimento dos números imaginários).
- Só era necessário prova para os n primos.
- Morreu vítima de um derrame, já cego.



Sophie Germain

- Tornou-se uma matemática profissional disfarçando-se de homem, para estudar na academia.
- Correspondia-se frequentemente com Gauss
- Provou para casos $n < 100$.
- Provou para todos os primos $2p+1$
- Morreu de câncer de mama aos 55 anos.
- Gauss escreveu: “inacreditável exemplo de uma mulher matemática”. E terminou dizendo “... nada poderia provar-me, de maneira tão lisonjeira e inequívoca”



Évariste Galois

- Matemático idealizador dos grupos.
- Firmou a Teoria de Galois, relacionando equações polinomiais.
- Aos 17 submeteu um artigo sobre solubilidade de equações na Academia Parisiense.
- As representações de Galois, que são fruto de sua Teoria, são ferramentas para a resolução de problemas até hoje.
- Morreu em 1832, aos 20 anos, após um duelo.



Paul Wolfskehl

- Industrialista com interesses em Matemática.
- Suicídio mal sucedido.
- Após sua morte, ofereceu um prêmio de 100.000 marcos para quem provasse que o “Teoama de Fermat” era verdadeiro, o chamado Prêmio Wolfskehl.



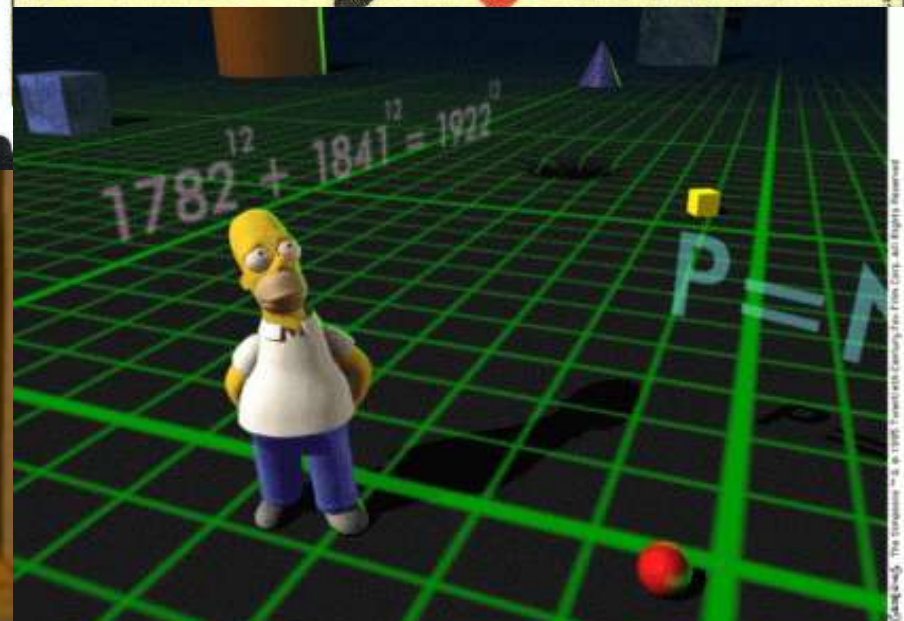
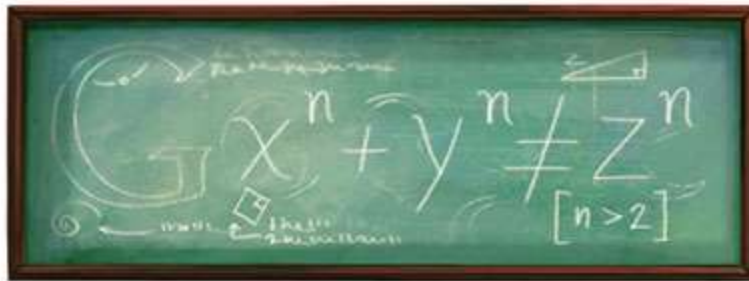
Yutaka Taniyama 谷山 豊

- Yutaka confirmou as propriedades das funções-L em curvas elípticas.
- Em parceria com Goro Shimura, criou a conjectura de Taniyama-Shimura, que afirma que **toda curva elíptica também é função modular**.
- Suicídio em 1958, por depressão.



Cultura Pop

- $1782^{12} + 1841^{12} = 1992^2$
- $3987^{12} + 4365^{12} = 4472^{12}$
- Star Trek – 22/03/1989 – “O problema continua sem solução após 800 anos”
- No Romance *Rocheworld* – 1960 – o problema permanece sem solução até que exploradores apresentam o problema a nativos de outra galáxia, que o resolvem rapidamente.



Testes computacionais

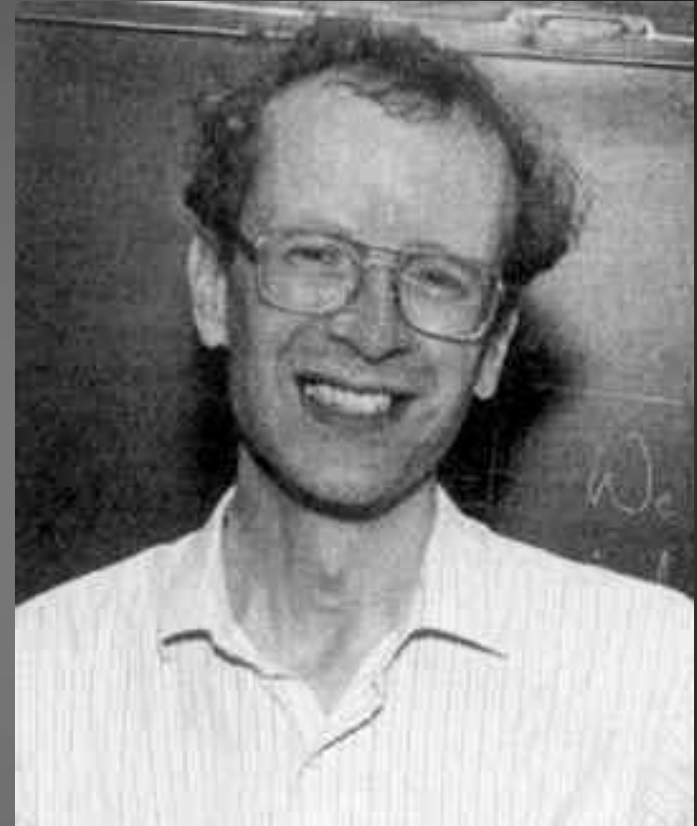
- Com o advento da computação, foi possível testar a conjectura para muitas entradas. Mas, ainda assim não era o suficiente para prová-lo verdadeiro.
- Existem alguns problemas em extrapolar resultados, como:
31, 331, 3.331, 33.331, 333.331, 3.333.331, 33.333.331 primo
Mas 333.333.331 é 17×19607843
- $X^4 + Y^4 + Z^4 = W^4$ (proposta por Euler)
Em 1988 encontraram :
 $2.682.440^4 + 15.365.639^4 + 18.796.760^4 = 20.615.673^4$

$$x^n + y^n \neq z^n$$

**E claro que é muito especial
porque Fermat disse que
tinha uma solução.**

Andre Wiles

- Conheceu o problema aos 10 anos
- Incentivado a abandonar o problema, passou a trabalhar com curvas elípticas.
- Passou 7 anos trabalhando em segredo absoluto, só dividindo seu trabalho com Nicholas Katz.
- Utilizou a conjectura epsilon para mostrar que a “curva de Fermat” não era modular.
- Provou particularidades da conjectura de Taniyama-Shimura.
- Aclamado cavaleiro do Império Britânico e recebeu quase todos possíveis prêmios. Matemáticos.





Descobri uma demonstração maravilhosa desta proposição que, no entanto, não cabe nas margens deste livro.



Uctv
DOCUMENTARY

us) All Elliphic
Curves are
Modular

Referências

- <http://fermatslasttheorem.blogspot.com.br/>
- [SINGH, Simon](#) (1998). *O último teorema de Fermat*. Rio de Janeiro: [Editora Record](#).
- http://www-history.mcs.st-and.ac.uk/HistTopics/Fermat%27s_last_theorem.html
- <http://www.cs.uleth.ca/~kaminski/esferm03.html>
- <http://www.cs.berkeley.edu/~anindya/fermat.pdf>

