Bll Journal Club (27 December 2002)

# The Saga of Fermat's Last Theorem

Presented by: Sandeep Somani

# What is it about ?

- A brief history of (pure) mathematics ...
- ... through the story of Fermat's Last Theorem ...
- ... the most baffling, tantalizing, intriguing problem of mathematics
- Based on the book Fermat's Last Theorem by Simon Singh

# Why this book ?

have ever read"

"This is probably the best popular account of a scientific topic I **RISH TIMES** 

- "To read it is to realize that there is a world of beauty and ٠ intellectual challenge that is denied to 99.9 per cent of us who are not high-level mathematicians" - THE TIMES
- "Reads like the chronicle e love affair. It has the would recognise" classic ingredients

- DAILY MAIL

# What's the problem ?!

- Question Time!!
- x + y = z
- $x^2 + y^2 = z^2$

infinite integer solutions  $\{(x,y,z)\} = \{(1,2,3); (10,40,50) \dots\}$ infinite integer solutions  $\{(x,y,z)\} = \{(3,4,5); (5,12,13) \dots\}$ 

•  $x^3 + y^3 = z^3$ 

NO integer solutions

•  $x^n + y^n = z^n$ 

*NO* integer solutions for all n>2

# .... the problem



## .... the problem



Figure 5. Is it possible to add the building blocks from one cube to another cube, to form a third, larger, cube? In this case a  $6 \times 6 \times 6$  cube added to an  $8 \times 8 \times 8$  cube does not have quite enough building blocks to form a  $9 \times 9 \times 9$  cube. There are 216 (6<sup>3</sup>) building blocks in the first cube, and 512 (8<sup>3</sup>) in the second. The total is 728 building blocks, which is 1 short of 9<sup>3</sup>.

# Who was Fermat ?!

- Pierre de Fermat was born on 20 Aug 1601 in S/W France to a wealthy leather merchant
- Due to pressure from family joined Civil Service
- "Prince of Amateur Mathematicians"
- Notorious!
   "Braggart" Rene Decartes
   "That damned Frenchman" John Wallis (Englishman)
   To Blaise Pascal "Whatever of my work is judged worthy of publication, I do not want my name to appear there"

# What did he do ?!

- Developed Probability Theory with Pascal
- Calculus
- Biggest Contribution was Number Theory
  - proved 26 is the only number sandwiched between a square and cube

- Friendly Numbers .. discovered second pair (17296,18416) after Pythagoras (220,284)

# Origin of the problem (some history) ..

600 BC

Pythagorean Brotherhood Proof, counting numbers

Alexandria Library

332 BC

Euclid Elements (second best seller after bible!) Irrational numbers, *reducio ad absurdum* 

250 AD Diophantus wrote *Arithmetica (13 vols)* 



389 ADFirst blow to Alexandrian library by Christian rulers642 ADSecond and final blow by Moslem ruler Omar Caliph~600 ADZero was discovered by Indians and Indo-Arabic notation became<br/>prevalent ie 155/601 instead of CLV/DCI !!

1601 AD 🦊 Fermat was born

6 volumes of Arithmetica survived and they were destined for the desk of Fermat

# Origin of the problem ...



Kune primum Greed es Latine editi, atque abfolutificais Commentariis illuftrati.

AVCTORE CLAVDIG GASPARE DACHETO MEZIRIACO SEEVITANO.4.C



LVTETIAE PARISIORVM; Sumpribus HIERONYMI DROVART, via lacobra, fub Scuto Solari. M. DC. XXI. CVM PRIVILEGIO REGIS: Luckily, The text had generous margins!

Bachet did a Latin translation of *Arithmatica* titled "Problems plaisans et delectables qui se font par les nombres" Having 100 problems in number theory with detailed solutions

# ... Fermat commented it !



## ...and the monster is created!

#### Arithmeticorum Liber II. 61

1 N. acque ideo institut 1 N. - 2. Oporter itaque 4 N. +4. triplos effe ad 2. & adhue superaddere 10. Ter igitur 2, adicitis vniratibus 10. æquatur 4 N. -> 4. & fis 1 N. 2. Erit ergo minor 3. maior 5. & farisfaciisnt qualtioni.

internallum numeroruma, minor anten et inte o des milles inu et inde al S. duithe des destants of upraduce of speakastices; is at A. & iss complexin at i. spis der periode (5 pt) pet i. ton water set & period J. z' phoney & algebrach set 7". Some & sain shinessur a 7. 6 of seifor a' 5. 2; series ad moolinera.

IN QUAESTIONEM VIL

CONDITIONIS spolite caden series ell que & opposite precedenti quefficoti , nil caim Galiad requinir quans ve quadratus successiti numerorum fie misse internalio quadratonum , & Capones idem hie etiam locum habebunt, et manifeftum eft.

#### QVESTIO VIII.

PROPOSITIVA quadrazum davidere in duos quadratos. Imperatum fit ve 16. diuidatur in duos quadratos. Ponatur primus i Q. Oporterigitur is - i Q. a quales effe quadrato. Fingo quadratum a numeris quorquot libnerit, cum defectu tot wnitestum qued continet latus iphus te. efte as N. - 4. ipfe igitor quadrants eric 4Q -+ 16.-16 N. has aquabunear voitanbus 16 - 2 Q. Communis adisciatur steinique de fectus, 8c a fimilibus auferantur fimilia, fient y Q. squales to N. & fir r N. " Eritiginn alter quadratorum W. alter vero # & strinfque fomma eff-1" feu 16. & vterque quadrance out

PTTON Straffala receive and alan in The respectations in manifes do to a Anterio eis d'un verpajamme. und veraigen a creptor dunament part. Store aca porddue of reider dividuous weat love of meverfinen miniare i vergiszerer Levis, imm dh mers Acid es moneuras bour leir à ir as is address. Too of f deblar at S. wirde des à midianes les duraper à pi mi reider of 15. min im porten of reider Surdune wer som merezadou à soite. n' bird breding Largen. Succession; and i long automic of . 13 giver of digedude of . wiper-Two isons bully not since or ison then is do good all ours die rac main



Hans marginis exiguitas non caperes.

#### QVASTIO IX.

Vasys oponeat quadratum 16 R diaidere in doos quadratos. Ponatur rurfus primi latus i N. alterius verò quoteunque numerorum com defectu tot vaitatum, quot conftat latus dividendi. Effo itaque a N. -4. crunt quadrati, hic quidem 1 Q. ille vero 4 Q. + 16. - 16 N. Carcrum volo vireinque fissul acquari vnitatibus 12. Igitot 5 Q. + 16. - 16 N. æquatur vnizaribus 16. & fit 1 N. Verit

TIT I of male vie a mepajaret di-Louis eis d'és revers sinous readifier mises i ni monierou mildogi (\* inic., i 3 ni iripa ci inne d'ances idelas ut inne iti i ni dingpueblie mid pai. The de et & nei for at \$. Forrer of a rerition and be aby Subauctor same, be J's Freedinger & at 15 robotes in 15. Rob-Asues The Sus Acener ourse Farme Town in at ef. Sundane des i ut it house et it long set if. nel giverne & acelaite if marellar. Hait

Cubem autem in duos cubos, aut Quadratoquadratum in duos quadra-Toquadratos, 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 caparet

#### i.e.

I have a truly marvelous demonstration of this proposition which this margin is too narrow to contain!!

### Why is it called the 'Last Theorem' ?

There were many such 'propositions' by Fermat

For eg: All primes can be written as 4p+1 or 4p-1Type 1 ie  $4p+1 = x^2 + y^2$  but not 4p-1

Euler proved this in 1749 after 7 years of work !

#### BUT

The "last" theorem could not be proved

### ... and the ordeal begins ...

1665

Death of Fermat

1753

Euler proved for n=3 based of Fermat's hint for n=4 case using method of infinite descent and imaginary numbers



### ... and the ordeal continues .

1665 1753 Death of Fermat Euler proved for n=3 based of Fermat's hint for n=4 case using method of infinite descent

1776 Birth of Sophie Germain (aka Monsieur Le Blanc) Considered the rost Illiant French woman ever Story time! Germain Primes, (1794) Ecole Polytechnique, (1806) Gauss, Lagrang Pg 112

1825

Gustav Lejune Dirichlet & Adrien-Marie Legendre

Independently showed n = 5









Note: Only Prime *n* need to be considered

#### ... the ordeal continues ...

- 1665 Death of Fermat
- 1753 Euler proved for n=3 based of Fermat's hint for n=4
- 1776 Birth of Sophie Germain
- 1825 Dirichlet & Adrien-Marie Legendre (n = 5)
- **1839** Another French **Gabriel Lame** did n = 7
  - Cauchy vs Lame

1847



German Ernst Kummer ... Unique factorization (by Euclid) irregular primes (37,59,67) were the problem A BIG BLOW (pg 128)!



# Fast Forward >>

- Andrew Wiles, was born on 11 April, 1953 at Cambridge, UK
- Stumbled upon Fermat's Last Theorem when he was 10 and tried to prove it then
- Studied Euler, Germain, Cauchy, Lame', Kummer and hit the same wall as Kummer
- Phd in Elliptic Equations
   y<sup>2</sup> = x<sup>3</sup> + ax<sup>2</sup> + bx + c
   a = 0, b = 0, c = -2 case was solved by Fermat
- Migrated to Princeton in 1980s
- In 1993 (almost) presented the solution to Fermat's Equation at Newton Institute, Cambridge



#### Back to our story ...

1847

Cauchy vs Lame and Kummer's Wall

A long gap of indifference

1908

Paul Wolfskehl, A German Industrialist rejevunated the quest

Story Time!! Love, Suicide, Award, Landau (1909-34).. Univ of Gottingen (Pg-144)

### the story continues ...

1847 1908 ~**1900**  Cauchy vs Lame and Kummer's Wall Paul Wolfskehl, A German Industrialist rejevuna

Hilbert Program was started by the Mathematical Logicians

Proving laws like Law of Trichotomy

and defining things like 'threeness' (pg 150)

Story Time!! Defn of Logic Bertrand Russel's paradox (pg 154)

1931

Kurt Godel, a Czech mathematician gave his *Theorem's of Indecidability !* something like: "I am a liar"

"This statement does not have any Proo

IMPLICATION: Certain theorems might be true but there may not be any way of proving them ...... and Fermat's Last Theorem might be one of them !





#### The quest continues ...

1847 1908 1931 Cauchy vs Lame and Kummer's Wall Paul Wolfskehl, A German Industrialist rejevunated the quest Kurt Godel, a Czech mathematician gave his

~1950

After Second world war computers were used to implement Brute Force Method Alan Turing was involved in it Demonstrated for n < 10000 ~1980 At Univ of Illinois n < 25000 more recently n < 4 million !!

#### Interesting facts

•31,331,3331, ..., 33 333 331 are all primes BUT 333 333 331 = 17 x 19607843 !!

•Euler Conjecture

 $x^4 + y^4 + z^4 = w^4$  has no integer solution BUT in 1988 Naom Elkies at Harward found one (pg 178) !!

### The quest continues ...

1955

1984

Cauchy vs Lame and Kummer's Wall Paul Wolfskehl, A German Industrialist rejevunated the quest Kurt Godel, a Czech mathematician gave his Brute Force Method

Taniyama-Shimura Conjecturestated the Equivalence of Modular forms andElliptic curves (whatever that means!)

*This was a mammoth idea (pg 211) Grand Unification Scheme by Langlands* 

Gerhard Frey claimed:
"Proof of T-S will immediately prove Fermat's Last theorem"
Also
"If Fermat's theorem is wrong so is T-S and that would be disastrous"





The most important problem in mathematics of 17<sup>th</sup> century got linked to most important problem of 20<sup>th</sup> century!

### Finally ... the quest concludes !

Kurt Godel, a Czech mathematician gave his Brute Force Method Taniyama-Shimura Conjecture Gerhard Frey

Andrew Wiles started working to prove T-S conjecture

pg 223 Ken Ribet, Barry Mazur, Evariste Galois

1993

1986

1995

Andrew Wiles presented the proof of T-S conjecture ... Almost!!

Andrew Wiles completed the proof of T-S conjecture ... Conclusively

### "I think I will stop here"



• 3 Lectures 21-23 June 1993 at the Newton Institute

- The Lecture of the Century
- 180 page proof in the Annals of Mathematics (May 1995)



# My Comments !

# "I think I'll stop here";)

# Wish You a Happy New Year !

#### Questions ?!