

# Fermat's Last Theorem

# Fermat's Last Theorem

- After Fermat's death, his son went through his notes.
- In 1670 Fermat's son Samuel published a new edition of Diophantus including his father's notes.
- One of the problems in Diophantus said  
write a given square as the sum of two squares.
- Fermat wrote a note next to this problem saying it is impossible, in general, to divide any power beyond the square into powers of the same degree, but the proof he found is too large for the margin of the page.
- Fermat's Last Theorem : There is no solution to

$$x^n + y^n = z^n \quad \text{when } n > 2$$

# No one cares

- No one was interested in Fermat's work with numbers for quite a while.
- About 100 years goes by before anyone makes any effort to work with Fermat's Theorem.

# Euler's contribution

- In the 18<sup>th</sup> century Euler went through Fermat's number theory.
- He organized Fermat's work and found proofs for most of the claims Fermat made.
- In fact Euler only found one mistake Fermat had made in all of his notes.
- Later Euler proved the case when  $n=3$ , but since his proof for it was very different than the proof for  $n=4$ , which was proven during Fermat's lifetime, he couldn't use it to find a general proof.

# Early 19<sup>th</sup> century

- In the early 19<sup>th</sup> century several mathematicians made small contributions to the problem
- It was clear that proving the case for  $n$  prime would be enough to prove the theorem

$$(x^q)^p + (y^q)^p = (z^q)^p$$

# Germain

- The most important contribution in the 19<sup>th</sup> century was made by Sophie Germain
- Germain looked at the problem split into two cases
  - Case 1:  $x$ ,  $y$ , and  $z$  are not divisible by  $n$
  - Case 2: one of  $x$ ,  $y$ , or  $z$  is divisible by  $n$

# Germain cont'd

- Germain was the first person to show any general results
- She showed that the first case is true if  $n$  is prime, and  $2n+1$  is prime
- That is if  $n$  is prime, and  $2n+1$  is prime, then FLT is true when  $x$ ,  $y$ , and  $z$  are not divisible by  $n$
- This eventually led to the proof of the first case of FLT for all  $n$  up to 100
- In the 19<sup>th</sup> century it was hard for women to get work published in mathematics, so Germain's theorem was first published in a book written by Legendre in 1808 with credit to Germain

# Other contributions

- Dirichlet found a partial proof for the second case for  $n=5$ .
- Legendre finished the proof.
- Lamé proved it for  $n=7$ .
- The method Lamé used to show it for  $n=7$  was difficult and not promising for larger numbers.
- A new method had to be found.



# Lame's mistake

- Lame thought of a new way to prove it.
- Lame decided to use complex numbers to factor the equation, and then wrote a proof based on that.
- One of the men reviewing his proof didn't know if complex numbers would share the same properties as other whole numbers, and so asked a fellow mathematician named Kummer.
- Kummer knew that they didn't necessarily share those properties, and therefore the proof was invalid.
- The problem drew Kummer's attention and he proved it for "regular primes".

# Kummer

- Regular primes are primes that do not divide the numerator of any Bernoulli number
- A Bernoulli number is in this form
- The only primes under 100 that aren't regular are 37, 59, and 67

$$B_n x^n / n!$$

# FLT is proven

- After Kummer's proof in 1847, very little headway was made
- In 1909, Paul Wolfskehl offered 100,000 marks to anyone who could find a proof which lasted until WWI when the mark became almost worthless
- People continued working on it but to no avail until 1993
- In 1993 Andrew Wiles announced that he found a proof for FLT
- He sent the proof to a journal which found a gap in the proof
- Several months later he had fixed the gap and had a correct proof to Fermat's Last Theorem

# Fermat's last tango

- Wiles said that the first six years working on the proof were enjoyable, but the last few months trying to fix the gap in the proof were terrible.
- There was a musical play about Wiles' struggle to finish the proof called Fermat's last tango.
- It took more than 300 years to prove Fermat's Last Theorem

# Timeline

- Fermat lived 1601 – 1665
- Marginal note stating Fermat's Last Theorem 1630
- Euler shows for  $n=3$  1770
- Sophie Germain found first general results 1808
- Dirichlet and Legendre proved FLT for  $n=5$  1825
- Lamé proved FLT for  $n=7$  1839
- Kummer proved FLT for "regular primes" 1847
- Paul Wolfskehl offered 100,000 Dm reward 1909
- Andrew Wiles proved FLT 1993-1994

# References

- O'Connor, J. Robertson, F. "Fermat's last theorem" February, 1996  
[http://www-groups.dcs.st-and.ac.uk/~history/HistTopics/Fermat's\\_last\\_theorem.html](http://www-groups.dcs.st-and.ac.uk/~history/HistTopics/Fermat's_last_theorem.html)