ON FERMAT’S LAST THEOREM

John Smith

In 1986 AndrewWiles published a ground-breaking proof of Fermat’s Last Theorem. But in spite of the rarity and the significance of the achievement, the underlying reasoning is so convoluted that it would be be extremely difficult -if not impossible- for any but a tiny minority of specialists to understand it. Most must simply take the word of Wiles and his fellow experts that Fermat’s Last Theorem has been proved. But the conjecture itself -that no 3 positive integers can satisfy the equation *x^n + y^n = z^n* for any positive-integer value of *n* greater than 2- is so simple that a school child could understand it, and Fermat himself claimed that he possessed a proof, one that -if it existed- must have been expressed in the language of 17th century mathematics, and the language of 21st century high school mathematics. Ye there can be no such proof: this note outlines a complimentary but alternative argument to that employed by Wiles that shows why no 17th century proof of the theorem is possible.

Andrew Wiles’ proof of Fermat’s Last Theorem

In 1637, Pierre De Fermat claimed that no 3 positive integers can satisfy the equation *x^n + y^n = z^n* for any positive-integer value of *n* greater than 2. More than 300 years later in 1986, British mathematician Andrew Wiles completed a childhood dream to prove what had come to be known as 'Fermat's Last Theorem' by use of the following general argument:

- All elliptic curves are modular (The Taniyama-Shimura Conjecture);
- If there are any positive-integer solutions to Fermat’s equation greater then 2, then this solution would be associated with an elliptic curve (The Frey curve) which is non-modular;
- Hence there are no such solutions.

Although Wile's proof is a tremendous achievement in the sense that Andrew tackled a 300 year old problem and came up with the solution where all before him had failed, it is lacking in elegance and simplicity. It runs into 200 odd pages, uses almost every number-theoretic technique known to man, and is perhaps the most tortuous argument in the history of mathematics. In the end, the truth of Fermat's simple claim is left more or less unexplained, and it is inexplicable except to a very small number of specialists. Fermat maintained that he had a 'truly marvellous' proof of his theorem, and famously wrote in the margin of an edition of Diaphantus' *Arithmetica* that this was 'too small to contain it'. Any proof no doubt used 17th century mathematics, and would be within the grasp anyone who studied maths at high school. Professionals and amateurs have tried over the centuries to find a proof that might have been Fermat's, and an several fictional amateurs have been in possession of short proofs: Lisbeth Salander, the central character in the trilogy of crime novels by Stieg Larsson known as the Millennium series apparently discovered Fermat’s original proof, and the Doctor in the episode of the TV series *Dr Who* called “The Eleventh Hour” types the original proof in a few seconds on a laptop’ -together with an explanation of why electrons have mass, and how superluminal travel is possible- to prove to the world that he is its savior. Unfortunately the writers failed to provide any details of these ‘proofs’, albeit that they had the space to do so. To see that there is *no* possibility that Fermat had a proof of his theorem, nor any possibility that such a proof could be presented using 17th century mathematics, consider the following general approach to the problem...

Fermat’s Last Theorem Revisted

This alternative approach to Fermat’s Last Theorem considers objects governed by the equation

$$\lim_{x\to\infty} e^{(s+1)\left(\zeta(s)-\frac{1}{s-1}\right)}\left(\left(\frac{1}{\exp\left((s+1)\left(\sum_{n=1}^{x}\frac{1}{n^s}-\int_1^x\frac{1}{n^s}\,dn\right)\right)}\right)^{\frac{1}{s+1}}\right)^{s+1} = 1$$

If we identify positive-integer solutions to Fermat's equation greater than 2 with real values of $s \neq 1$ and finite arithmetic progressions, then we may form the following argument:

- Where s is a real number other than 1, all objects governed by the equation above are associated with finite arithmetic progressions and hence with a finite numbers of primes;
- If there are any positive-integer solutions to Fermat’s equation greater then 2, then this solution would be associated with a real value of $s \neq 1$ and a potentially infinite arithmetic progression, and thus with a potentially infinite number of primes;
- Therefore there are no such solutions.

Linking with Wiles’ argument:

- Every modular form is associated with an L-function;
- Every L-Function is associated with a potentially infinite number of primes;
- If and only if $s = 1$, is an L-Function associated with a potentially infinite number of primes;
- If there are any positive integer solutions to Fermat’s equation greater then 2, then there are a potentially infinite number of primes associated with an L-Function in the case that s is a real number other than 1;
- Therefore there are no such solutions.

Fermat’s Last Theorem concerns the equation for the circle, and $\lim_{x\to\infty} e^{(s+1)\left(\zeta(s)-\frac{1}{s-1}\right)} \left(\left(\frac{1}{\exp\left((s+1)\left(\sum_{n=1}^{x}\frac{1}{n^s}-\int_1^x \frac{1}{n^s}\,dn\right)\right)}\right)^{\frac{1}{s+1}}\right)^{s+1} = 1$ concerns the ways in which π -in the sense of the ratio of a circle’s circumference to its diameter- can be distorted. This theorem, together with the Riemann Hypothesis, the Poincare Conjecture, the Birch and Swinnerton-Dyer Conjecture, is placing limits on how great this distortion can be before a manifold ceases to be smooth, in which case it ceases to be Euclidean. Given that *non-Euclidean* geometry was not discovered until the 19th century, and that Fermat’s Last Theorem cannot be proved without direct or indirect appeal to non-Euclidean geometry, a 17th century proof of the theorem is to be deemed impossible.

REFERENCES

Diaphantus (1621), *Arithmetica*

Larsson, S (2015), *The Girl Who Played With Fire*

Singh, Simon (1997), *Fermat’s Last Theorem*

Wiles, A (1995), Modular elliptic curves and Fermat's Last Theorem