The Hunting of Another Snark

$$a^n + b^n = c^n$$

Tony Thomas

The Hunting of Another Snark

No one knows whether Pierre de Fermat really did have a proof of his famous conjecture that would justify it being called a theorem. However, he declared that he did in his copy of Diophantus' Arithmetica. The original copy was lost but the marginalia was reported by his son to be as follows.

It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second into two like powers. I have discovered a truly marvellous proof of this, which this margin is too narrow to contain.

It would be churlish to suppose that Fermat had no genuine proof, but it is strange that no record of such a proof exists other than his provocative marginal note. Over 350 years elapsed before Andrew Wiles produced his complex proof of Fermat's conjecture, and this was only achieved after years of research into the problem. Wiles's proof is difficult and draws upon several esoteric branches of mathematics. This renders it incomprehensible to all but the highly trained mathematician. Unfortunately I am not among these.

Fermat's conjecture appears to be very simple, and states that the sum of two integral numbers raised to a third or higher power can never equal an integer raised to the same power ie $a^n + b^n \neq c^n$ when $n > 2$. This qualification is necessary because there are infinitely many solution to the equation when $n = 2$. In other words there are innumerable examples of Pythagorean triangles with three integral sides. The simplest of these is the (3,4,5) triangle, which was known to the Babylonians.

Fermat's conjecture applies to all dimensions higher than two and it is disappointing that no examples of $a^n + b^n = c^n$ have ever been discovered for dimensions higher than two. A cursory examination of the problem soon convinces the enquirer that it is unlikely that there could be any solutions, but proving that this is so requires more than familiarity with the problem and mere intuition.

The conjecture poses a unique problem because it seeks to prove a negative: that there are no solutions to the equation. Searching for a needle in a haystack is difficult enough but becomes nigh on impossible when the haystack is infinite. However, proving there is no needle raises the problem to a still higher level.

In his poem, *The Hunting of the Snark*, Lewis Carrol seems to wrestle with a similar problem. A group of bumbling adventurers sets out in a boat (with the bowsprit on the stern) in search of a mythical but deadly creature: the Snark. The journey is fraught with dangers, including encounters with the Jubjub, the Bandersnatch and possibly the Boojum. Such fabulous creatures are reminiscent of the strange mathematical forms that arise in pursuit of the theorem that would prove Fermat's conjecture true.

Among these hazards are fallacies, facile assumptions, misconceptions, transcription errors and the confusion of one symbol with another, not to speak of downright blunders of the crudest kind. The imagination and creative intuition flies forward at lightning speed, leaving a trail of errors in its wake. Triumphant sightings of the Snark inevitably turn out to be a Boojum. Lewis Carrol might well have named some of these creatures as 'fallunders', blundacies' or 'crudumptions' according to his theory of portmanteau words with joint meanings.

Fermat's conjecture poses an intractable problem, like a smooth cliff face that offers the climber no safe handhold. Expanding the original form into a more elaborate one provides plenty of scope for beginning the climb towards the inaccessible peak of the solution. The binomial theorem is an obvious route but one that soon leads into a wilderness of ever increasing complexity.

For the beginner, a useful preliminary is to study the Pythagorean forms in detail ie the solutions to $a^2 + b^2 = c^2$. The basic (3,4,5) triangle is not alone: for every odd number there is a solution that is easy to calculate. Examples of these 'primitive' forms are (3,4,5), (5,12,13), (7,24,25), (9,40,41) etc. Each of these forms can be multiplied without limit to provide an infinite number of solutions eg (6,8,10), (9,12,15) etc. This fundamental principle means that the existence of a single primitive solution for $n > 2$ implies the existence of infinitely many solutions. The failure to detect any solutions strongly suggests that the Snark is well hidden in its infinite maze.

This process of enquiry reveals the principles that would have to apply to higher dimensions. For example, the primitive forms must be (odd,even,odd) and the only possible alternative is (even,even,even). This simple notion of parity consistency (odd + odd = even) and (even + even = even) leads on to the more complex idea of how numbers combine according to the residues generated by moduli higher than 2. Choosing a line of enquiry to pursue holds out the prospect of a wrong direction that could involve years of wasted time or a quick route to a solution.

The brute force of the computer provides empirical evidence that $a^n + b^n \neq c^n$, although many of the results are tantalisingly close. However, the computer's power is soon overcome as its capacity to deal with large numbers becomes exhausted. The refinements of logic and mathematics cannot be replaced by technology, but the computer is useful for presenting patterns to the eye that may not be evident to the unaided intellect.

Adopting many lines of enquiry and gathering insights along the way is an invaluable process. Einstein's aphorism, "imagination is more important than knowledge" lies at the heart of the creative process although little progress can be made without a sufficient understanding of mathematics and logic. Devising solutions to Fermat's conjecture has long been the hobby of cranks and incompetent mathematical amateurs. The number of erroneous solutions has multiplied exponentially over the centuries and contributions by eccentric geniuses continue to plague mathematics departments around the world.

This poses a dilemma for the dedicated hunter of the Snark. Should the enquirer who has survived the clutches of the Bandersnatch and the Jubjub bird continue with the search, despite the continual transformation of the elusive Snark into the ubiquitous Boojum or give up the hunt knowing that no one would believe that another Snark had been captured and rendered harmless. Even having the Snark in one's clutches would expose the hunter to the ridicule of real mathematicians who know that the only one in existence has already been captured by Andrew Wiles, and lies caged somewhere in Princeton University. If it walks like a Snark, and quarks like a Snark it may well be a Snark, so without further ado I offer the Boojum below for your tender consideration.

Fermat's Last 'Theorem'

It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second into two like powers. I have discovered a truly marvellous proof of this, which this margin is too narrow to contain.
Pierre de Fermat

THE APPLICATION OF PYTHAGOREAN TRIPLES TO FERMAT'S EQUATION

TONY THOMAS

Part I of this paper defines two generating functions for Pythagorean triples and extends the definition of Pythagorean triples to irrational numbers. Part II applies the attributes of Pythagorean triples to Fermat's equation when the exponent is an odd number. Part III applies the attributes to Fermat's equation when the exponent is an even number. A proof of Fermat's conjecture was published by Andrew Wiles in *Annals of Mathematics, 1995*. The proofs in Parts II and III provide an alternative but shorter proof of Fermat's Conjecture.

Part I - Pythagorean Triples

A Pythagorean triple is a set of three integers (α, β, γ) such that $\alpha^2 + \beta^2 = \gamma^2$.

A subclass of the Pythagorean triples is defined when α, β and γ have no common factor. This subclass contains primitive solutions to Pythagoras's Theorem and its members will be denoted by the term 'primitive triples'. The remaining solutions are defined by $(\lambda\alpha, \lambda\beta, \lambda\gamma)$ where $\lambda \in N$ and $\lambda > 1$.

Generating functions can be defined for the set (α, β, γ) in terms of α, which by convention is the least member of the set. However, there is a transient exception to this when $\alpha = 2$, so the set is restricted by the condition $\alpha > 2$. For convenience, separate generating functions are defined for odd and even values of α. These functions are:

$GF1: [a, (a^2-1)/2, (a2 + 1)/2]$ defines (α, β, γ) for the odd values of a and

$GF2: [a, (a^2-1), (a2 + 1)]$ defines (α, β, γ) for the even values of a.

Each function imposes the following attributes on (α, β, γ):

$$GF1: \Rightarrow \alpha^2 + \beta^2 \neq \gamma^2 \wedge \beta + \gamma = \alpha^2 \wedge \beta - \gamma = 1$$
$$GF2: \Rightarrow \alpha^2 + \beta^2 \neq \gamma^2 \wedge \beta + \gamma = \alpha^2/2 \wedge \beta - \gamma = 2$$

The primitive triples have been defined as integers, but the generating functions can take up rational and irrational values of a. When a is a real number, the attributes of the primitive triple (α, β, γ) remain unchanged under the generating functions.

Since it is the attributes that will used in the proof of Fermat's conjecture, the assignment of irrational values to a is therefore warranted. The values concerned will be restricted to square roots, which is relevant for the resulting values of β and γ.

When $a^{1/2}$ is substituted into *GF1* and a has no square root, α will be irrational but β and γ will be rational fractions if $a \nmid 2$.

LEMMA 1

If (α, β, γ) is a primitive triple as defined above then $\beta - \gamma = 1 \vee \beta - \gamma = 2$.

LEMMA 2

$$n > 2 \wedge p < q \Rightarrow q^n - p^n > 2$$

Part II – Fermat's Equation with Even Exponent

Fermat's conjecture can be expressed as follows:

$$a^n + b^n \neq c^n \qquad (a, b, c, n \in N), (a < b < c), (n > 2)$$

In seeking to prove this conjecture, which is denoted here by FLT, the contrary assumption ~FLT is made in order to establish FLT *reductio ad absurdum*.

Restating the conjecture in contrary form:

$$\sim FLT: a^n + b^n = c^n \qquad (a, b, c, n \in N), (a < b < c), (n > 2)$$

A further condition is that a, b and c have no common factor so that only primitive solutions need be considered.

If it is the case that $A^n + B^n = C^n$ has a maximum common factor f, then defining $A/f = a$, $B/f = b$, and $C/f = c$ produces the required condition that a, b and c have no common factor.

LEMMA 3

Let $X = a^{n/2}$, $Y = b^{n/2}$, and $Z = c^{n/2}$ $\qquad (X, Y, Z \in R)$

$$X^2 + Y^2 = Z^2 \Rightarrow Z - Y = 1 \vee Z - Y = 2$$

PROOF:

Since a, b and c have no common factor by definition it follows from the definitions of X, Y and Z that X, Y and Z have no common factors, at least when they are integers. If $X^2 + Y^2 = Z^2$ then (X, Y, Z) is a primitive Pythagorean triple as extended to real numbers. It follows from Lemma 1 that $Z - Y = 1 \vee Z - Y = 2$.

PROOF OF FERMAT'S CONJECTURE FOR EVEN EXPONENT

Suppose $a^n + b^n = c^n$

Let $X = a^{n/2}$, $Y = b^{n/2}$, and $Z = c^{n/2}$ $(a, b, c, n \in N), (n > 2), (n|2)$

So $(a^{n/2})^2 + (b^{n/2})^2 = (c^{n/2})^2 \Leftrightarrow a^n + b^n = c^n$

And $a^n + b^n = c^n \Leftrightarrow X^2 + Y^2 = Z^2$

Now $X^2 + Y^2 = Z^2 \Rightarrow Z - Y = 1 \vee Z - Y = 2$ according to lemma 3

But $Y = b^{n/2}$ and $Z = c^{n/2}$

And $n > 2 \wedge p < q \Rightarrow q^n - p^n > 2$ according to lemma 2

So that $c^{n/2} - b^{n/2} > 2$

Therefore (X,Y,Z) cannot be a Pythagorean triple

And $X^2 + Y^2 \neq Z^2$

Consequently $a^n + b^n \neq c^n$ *reductio ad absurdum*.

THEOREM $a^n + b^n \neq c^n$ $(a, b, c, n \in N), (a < b < c), (n > 2)\ (n|2)$

Part III – Fermat's Equation with Odd Exponent

PROOF OF FERMAT'S CONJECTURE FOR ODD EXPONENT

When n is an odd number with no square root, X, Y and Z are irrational numbers under the definition $X = a^{n/2}$, $Y = b^{n/2}$, *and* $Z = c^{n/2}$. However, when X is applied to the generating function *GF1* (or *GF2)* the resulting values of Y and Z are rational fractions.

Let (X, Y_1, Y_2) be the Pythagorean triple defined by X under *GF1* so that:

$$(X, Y_1, Y_2) = [a^{n/2}, (a^n-1)/2, (a^n + 1)/2]$$

Although X remains irrational Y_1 and Y_2 are rational. Furthermore:

$$Y_2 - Y_1 = 1$$

But $(X, Y, Z) = (a^{n/2}, b^{n/2}, c^{n/2)})$.

Since $X^2 + Y^2 = Z^2$ there must be a triple with X as the least term that satisfies this relation. (X, Y_1, Y_2) is a triple that satisfies the equality $X^2 + Y^2 = Z^2$.

Now (X, Y, Z) has the property $Z – Y > 2$ since $c^{n/}2 - b^{n/2} > 2$, when n > 2

So $(X, Y, Z) \neq (X, Y_1, Y_2)$

Since there can only be one triple containing the least term X which satisfies $X^2 + Y^2 = Z^2$, (X, Y_1, Y_2) must be that triple.

Consequently $X^2 + Y^2 \neq Z^2$

And $a^n + b^n \neq c^n$ *reductio ad absurdum.*

THEOREM $\boldsymbol{a^n + b^n \neq c^n}$ $\boldsymbol{(a, b, c, n \in N), (a < b < c), (n > 2) (n \nmid 2)}$

The Proofs in Part II and Part III constitute a proof of Fermat's Conjecture.

THEOREM $\boldsymbol{a^n + b^n \neq c^n}$ $\boldsymbol{(a, b, c, n \in N), (a < b < c), (n > 2)}$