THE REDISCOVERED PROOF OF FERMAT'S LAST THEOREM

A SYNOPSIS AT PRINCETON UNIVERSITY, NJ, USA
2015

1. Background

In 1995, Princeton professor Andrew Wiles quenched the quest for a proof of Fermat's last theorem as he accomplished the task in his 109-page tome *Modular Elliptic Curves and Fermat's Last Theorem* [1]. However, Fermat's "truly marvelous proof," which the margin of his copy of the *Arithmetica* was "too narrow to contain," has remained unknown. By Wiles's own admission, his proof, which involves such modern mathematics as the category of schemes and Iwasawa theory, could not have been the proof Fermat had in mind.

The most recent additions to our Seeley G. Mudd Manuscript Library feature contributions from the estate of Oliver Wendell Holmes, Jr., which include letters and legal manuscripts of Pierre de Fermat (a lawyer by vocation). It is in the density of Fermat's litigation records during the period 1660-1662 that his lost mathematical proof is finally to be found.

It turns out that Fermat's proof employs what is now known as the Mason-Stothers theorem (proved independently by Stothers [2] and Mason [3] in the late 20th century). In the discovered manuscript, Fermat himself gave an elementary proof of the Mason-Stothers theorem, but his approach resembles that presented in *An alternate proof of Mason's theorem* by Snyder [4]. For this reason we here omit Fermat's proof of the Mason-Stothers theorem, and only reproduce the subsequent part of his proof of his last theorem, paraphrased in modern terminology.

2. A Reproduction of Fermat's Proof

Theorem. *For any positive integer $n \geq 3$, there do not exist positive integers x, y and z, with $x, y, z \neq 0$, satisfying the equation*

$$x^n + y^n = z^n.$$

Proof. We shall invoke the following theorem proved by W. Wilson Stothers [2] and R. C. Mason [3].
Theorem (Mason-Stothers)**.** *For any polynomials $A(t)$, $B(t)$ and $C(t)$, with complex coefficients, satisfying $A + B = C$,*

$$\max\{\deg A, \deg B, \deg C\} \leq N(ABC) - 1,$$

where $N(f)$ is the number of distinct roots of f.

Now, suppose there is a solution to the equation $x^n + y^n = z^n$, where x, y and z are integers with $x, y, z \neq 0$, and n is a positive integer. Then $(xt)^n + (yt)^n = (zt)^n$, and hence

$$(xt)^n + (yt)^n + (\epsilon zt)^n = 0,$$

where ϵ is a complex number satisfying $\epsilon^n = -1$. Thus there exist polynomials $X(t)$, $Y(t)$ and $Z(t)$, with complex coefficients, satisfying $X^n + Y^n + Z^n = 0$, where $\deg X, \deg Y, \deg Z \geq 1$ (since $x, y, z \neq 0$).

By the Mason-Stothers theorem, $\deg X^n \leq N(X^nY^nZ^n) - 1$. But note that $\deg X^n = n \deg X$ and $N(X^nY^nZ^n) = N(XYZ)$ (for a number is a root of XYZ if and only if it is a root of $(XYZ)^n$). Hence

$$n \deg X \leq N(XYZ) - 1 \leq \deg(XYZ) - 1 = \deg X + \deg Y + \deg Z - 1.$$

Similarly we may obtain $n \deg Y \leq \deg X + \deg Y + \deg Z - 1$ and $n \deg Z \leq \deg X + \deg Y + \deg Z - 1$. Adding the three equations, we have

$$n(\deg X + \deg Y + \deg Z) \leq 3(\deg X + \deg Y + \deg Z) - 3,$$

or

$$(3 - n)(\deg X + \deg Y + \deg Z) \geq 3.$$

Since $\deg X, \deg Y, \deg Z \geq 1$, we must have $3 - n > 0$, i.e. $n < 3$. □

3. Remarks

Indeed, the course of true mathematics never did run smooth. The patient reader is wished a happy April Fools' Day. It is the sincere hope of the Organising Committee of the 57th International Mathematical Olympiad 2016, Hong Kong, that the falsity of this note will not discourage the reader from joining the search for beautiful solutions to hard mathematical problems.

References

[1] Wiles, Andrew (1995), *Modular Elliptic Curves and Fermat's Last Theorem*, Annals of Math. 141 (3): 443-551.
[2] Stothers, W. W. (1981), *Polynomial identities and hauptmoduln*, Quaterly J. Math. Oxford 2 (32): 349-370.
[3] Mason R. C. (1984), *Diophantine Equations over Function Fields*, London Math. Soc. Lecture Note Series 96, Cambridge, England: Cambridge University Press.
[4] Snyder, Noah (1999), *An alternate proof of Mason's theorem*, Elemente Mathematik 55 (2000), no. 3, 93-94.