FERMAT'S PROOF OF HIS LAST THEOREM: AN ENLIGHTENING NOTE ON TRANSITIVE INEQUALITY

ALLEN D. ALLEN†

ABSTRACT. By proving that his "last theorem" (FLT) is true for the integral exponent $n = 3$, Fermat took the first step in a standard method of proving that there exists no greatest lower bound on n for which FLT is true, thus proving the theorem. Unfortunately, there are two reasons why the standard method of proof is not available for FLT. First, transitive inequality lies at the heart of that method. Secondly, FLT admits to a condition in which $>$ changes to $<$ so their transitive properties cannot be used. FLT implies that for an integral exponent n, the inequality changes over the interval with the minimum extent $1 \leq n \leq 3$. For any exponent in the positive real numbers, a solution to Fermat's equation occurs and inequality is replaced by equality at the instant when four distinct exponential curves collapse into two intersecting curves.

---

†The author is retired from CytoDyn, Inc., Vancouver, WA, USA.
E-mail: **allend.allen@yahoo.com**
2010 MSC: Primary 03F07, 11D41, 65L10; secondary 01A45.

1. INTRODUCTION

Pierre de Fermat had a copy of Bachet's 1621 translation of *Arithmetica* by Diophantus of Alexandria [C]. Problem 8 of Book II of *Arithmetica* asks how to divide a given square number into two squares. In the late 1630s while pondering this problem, Fermat [H] wrote in the margin, "On the other hand, it is impossible to separate a cube into two cubes, or a biquadrate into two bioquadrates, or generally any power except a square into two powers with the same exponent. I have discovered a truly marvelous proof of this, which however the margin is not large enough to contain."

Fermat never published his "truly marvelous proof" of what became known as Fermat's Last Theorem (FLT). But he did prove that FLT is true for the integral exponent $n = 3$. In doing so, he took the first step in a standard method of proving that there exists no greatest lower bound on n for which FLT is true, thus proving FLT. That standard method of proof (SMOP) goes all the way back to Euler.[1] Either Fermat never knew this or he realized there was a reason SMOP is not available for FLT. Some such thing surely happened because Fermat went on to prove that FLT is true for $n = 4$, which was redundant and unnecessary for purposes of SMOP, a method based on the axiom that the positive integers are closed under addition.

Theorem 1.1 (SMOP). *Let* P(n) *be a proposition on the real numbers the truth of which depends upon positive integer* n. *Prove there exists a fixed positive integer* k *such that* P(k) *is true. Prove that if* P(n) *is true, then* P(n + 1) *is true*. *It follows that* P(n) *is true for all* $n \geq k$.

Over the ensuing centuries, the greatest known lower bound on the exponent n for which FLT was shown to be true grew in magnitude. The challenge became one of proving FLT for larger and larger exponents. But this goes in the wrong direction for SMOP, logically speaking. To prove FLT is valid across the entire countably infinite set of positive integers using SMOP, one shows that there exists no greatest lower bound on n for which FLT is true.

The next section investigates what Fermat started, whether or not knowingly. It will be shown that SMOP is not available for FLT because transitive inequality lies at the heart of SMOP and FLT admits to a condition in which > changes to <. The circumstances of this change will be shown in detail.

2. CHASING THE STANDARD METHOD OF PROOF

Let $N = \{\text{the positive integers}\}$.

Let R be the set of all ordered pairs $[r,s]$ of reduced rational fractions $0 < r < s < 1$.

[1] See www.people.reed.edu/~jerry/131/nextprime.pdf

It is easily shown and well-known that the following theorem is equivalent to FLT as originally stated by Fermat for Diophantine equations.

Theorem 2.1 (FLT). *If* $2 < n$, *then* $r^n + s^n \neq 1$.

In order to prove theorem 2.1 using SMOP, it would need to be shown that if $r^n + s^n \neq 1$, then $r^{n+1} + s^{n+1} \neq 1$. The reason this is not the case becomes clear if the non-specific inequality $\neq$ in theorem 2.1 is bifurcated into the two specific inequalities.

Lemma 2.2. *If* $r^n + s^n < 1$, *then,* $r^{n+1} + s^{n+1} < 1$.
Proof. If $[r,s] \subset R$, then $r < 1$ and $s < 1$. Hence, $r^n r + s^n s < r^n + s^n < 1$.

Lemma 2.2 shows the case in which transitive inequality makes SMOP available. If the antecedent condition $r^n + s^n < 1$ were always true, then it could be easily proved that there exists no greatest lower bound on n for which theorem 2.1 is true. But that antecedent condition is not always true because it depends upon small bases and large exponents.

Lemma 2.3. *If* $r^n + s^n > 1$, *then* $r^{n+1} + s^{n+1}$ *may or may not be greater than unity*.
Proof. If $[r,s] \subset R$, then $r < 1$ and $s < 1$. Hence, $r^n r + s^n s < r^n + s^n > 1$.

Definitions 2.4. Boundary conditions.

Definition 2.4.1. Let $\alpha[r,s]$ be the largest element of N such that $r^n + s^n > 1$.

Definition 2.4.2. Let $\beta[r,s]$ be the smallest element of N such that $r^n + s^n < 1$.

Given $[r,s] \subset R$, the condition $r + s \leq 1$ implies $\alpha[r,s]$ does not exist. Theorem 2.1 can then be proved using SMOP as shown by lemma 2.2. Such a pair would, therefore, be irrelevant for the present purposes. Consequently, it is assumed throughout the sequel that $\alpha[r,s]$ exists. In any case, $\beta[r,s]$ exists because if $[r,s] \subset R$, then $r < 1$ and $s < 1$. Hence, the sum $r^n + s^n$ is strictly monotone decreasing as n, which grows without bound as $r^n + s^n$ approaches zero asymptotically and eventually must become less than unity.

3. Analysis of the Change in Inequality

For the purpose of investigating the change of inequality from > to <, begin with the following preliminaries.

Let $\mathfrak{N}$ = {the positive real numbers}.

Definitions 3.1. Exponential functions. Let it be understood that x is a variable element of $\mathfrak{R}$, and the functions f and g are single-valued mappings from $\mathfrak{R}$ into $\mathfrak{R}$.

Definition 3.1.1. $f(x) = r^x$.

Definition 3.1.2. $g(x) = s^x$.

Definitions 3.2. Intervals. Note that $\alpha[r,s] < \beta[r,s]$ by definitions 2.4.

Definition 3.2.1. $\Delta x[r,s]$ is the bounded interval $\alpha[r,s] \le x \le \beta[r,s]$.

Definition 3.2.2. $\delta x[r,s]$ is the unbounded interval $\alpha[r,s] < x < \beta[r,s]$.

The change in inequality takes place over the bounded interval $\Delta x[r,s]$ in the unbounded interval $\delta x[r,s]$ at the instant

$$f(x) + g(x) = 1. \tag{1}$$

The number of positive integers in the interval $\Delta x[r,s]$ is $\beta[r,s] - \alpha[r,s] + 1$. Hence, to have any positive integer in the interval $\delta x[r,s]$ the necessary and sufficient condition is that $\beta[r,s] - \alpha[r,s] \ge 2$. According to definitions 2.4, the first integral value for x is $\alpha[r,s] + 1$ and the last integral value for x is $\beta[r,s] - 1$. Iff $\beta[r,s] = \alpha[r,s] + 2$, then there is exactly one integer in the interval $\delta x[r,s]$. Hence,

Theorem 3.3. *FLT implies that if (1) has an integral exponent, then the interval over which the change in inequality occurs has the minimum extent,* $\Delta x[r,s] = [1,3]$.

Note that the converse of theorem 3.3 is not true because R contains pairs $[r,s]$ such that $r^2 + s^2 \ne 1$. In other words, theorem 3.3 is a consequence of FLT but is not equivalent to it.

Theorem 3.4. *At that one unique point where (1) is satisfied and inequality is replaced by equality, four distinct exponential curves collapse into two intersecting curves.*

Proof. If $f(x) + g(x) \ne 1$, then $f(x)$, $1 - f(x)$, $g(x)$ and $1 - g(x)$ are four distinct exponential functions with four distinct exponential curves inasmuch as they all have different first derivatives, $r^x \ln r$, $1 - r^x \ln r$, $s^x \ln s$, and $1 - s^x \ln s$. But if $f(x) + g(x) = 1$, then $r^x = 1 - s^x$ and $s^x = 1 - r^x$ so there are only two distinct curves that intersect.

4. Conclusions

It is taken for granted that Fermat never actually proved FLT because he never published such a proof. The particular reason for this failure is rarely asked, at least not out loud. Following the proof of FLT that Wiles [W] found with the help of Taylor [F], mathematicians have rarely asked why FLT was so difficult to prove given that it is, indeed, true. It seems sufficient to say it

was centuries before anyone proved FLT, and then the proof was a marvelous tome running over 200 pages and based on a complex argument involving modular elliptic curves.

To help understand the difficulty in proving FLT, the present paper demonstrates that SMOP is not available for FLT because inequalities change so their transitive natures cannot be applied. But for that reason, FLT would have been proved centuries ago, if not by Fermat in the late 1630s, then by Euler, who was born in April of 1707. A closer look at the situation reveals a consequence of FLT not equivalent to it: When exponents are integers, the change in inequality happens over the minimal interval $1 \leq n \leq 3$. The necessary and sufficient condition for having any positive real number as the exponent in Fermat's equation is that inequality is replaced by equality at the instant four distinct exponential curves collapse into two intersecting curves.

REFERENCES

[C] A. Cox , Introduction to Fermat's last theorem. *Amer. Math. Monthly* **101**, 1994, 3-14.

[F] G. Faltings, The Proof of Fermat's Last Theorem by R. Taylor and A.Wiles, *Notices Amer. Math. Soc.* **42,** 1995, 743-746

[H] T. Heath, *Diophantus of Alexandria*, Second Edition, Cambridge University Press, Cambridge, Cambridge, UK 1910. (Reprint by Dover Books, New York, NY 1964).

[W] A. Wiles, Modular Elliptic Curves and Fermat's Last Theorem**,** *Ann. of Math*. (2), **141**, 1995, 443-551.