THERE ARE INFINITELY MANY THEOREMS AS DIFFICULT TO PROVE AS FERMAT'S LAST THEOREM: A CHARACTERIZATION OF SUCH THEOREMS

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 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 change from > to < rendering their transitive natures unavailable. A related, self-evident symmetry illustrates another problem that would have plagued Fermat and centuries of successors. FLT asserts such a narrow proposition, it is difficult to find an antecedent while easy to find a non-equivalent consequence. For example, if FLT asserted that the exponent n is even, then FLT would be equivalent to the proposition that Fermat's equation has two solutions, one for positive bases and one for their negative counterparts. This could be addressed with conservative transformations. The example provided by FLT motivates the use of an early paper by the author to prove a theorem on theorems. The theorem on theorems demonstrates there are infinitely many theorems as difficult to prove as FLT.

---

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

Abstract contains exactly 200 words.
Manuscript runs six pages.

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, 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. 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. Moreover, a self-evident symmetry related to how inequalities change illustrates another problem that would have plagued Fermat. FLT asserts such a narrow proposition that it is difficult to find an antecedent while easy to a non-equivalent consequence. For example, if FLT had stated that the exponent n is even, then FLT would be equivalent to the proposition that Fermat's equation has two solutions, one for positive bases and one for their negative counterparts. This could at least be addressed by conservative transformations.

It would be instructive, and not just of historical interest, to know why Fermat was wrong in believing that he had a proof. Over the ensuing centuries there were surely other fine mathematicians, promising post-doctoral students and undergraduates who shared Fermat's experience. Even as of this writing the open-access preprint depositories are not wanting for authors who believe they have found a superior proof of FLT. The question of why becomes

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

especially pertinent now that there is the proof of FLT that Wiles [W] found with the help of Taylor [F], a marvelous tome running over 200 pages and based on a complex argument involving modular elliptic curves. The present note will help answer that question with formal proofs of the obstacles mentioned above. This, in turn, motivates a theorem on theorems demonstrating that there are infinitely many theorems as difficult to prove as FLT lying in wait for the community of mathematicians.

2. CHASING AN EARLY PROOF

Let N = {the positive integers}.

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

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* $n > 2$*, 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 $[r,s] \subsetneq R$, 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.

Theorem 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 $[r,s] \subsetneq R$, then $r < 1$ and $s < 1$. Hence, $r^n r + s^n s < r^n + s^n > 1$.

A self-evident symmetry related to how inequalities change illustrates another problem.

Lemma 2.4. *Consider the equation*

$$r^n + s^n = 1^n. \tag{1}$$

Iff n *is even, then (1) has another solution*,

$$(-r)^n + (-s)^n = (-1)^n. \tag{2}$$

Obviously,

Lemma 2.5. *FLT implies that Fermat's equation has the two solutions (1) and (2).*

On the other hand,

Lemma 2.6. *If Fermat's equation has the two solutions (1) and (2), this does not imply FLT.*

Proof. Let $n = 2k$, $k \in N - \{1\}$. Then (1) has the solution (2) but $n > 2$.

As a direct consequence of lemmas 2.5 and 2.6,

Theorem 2.7. The proposition that Fermat's equation has the two solutions (1) and (2) is a consequence of FLT but does not imply it.

This can be sharpened.

Lemma 2.8. *If* $m \in N - \{1\}$, *then* $m = \prod p_i \wedge \varepsilon_i$, *where the* p_i *are prime numbers and the* $\varepsilon_i \in N$ *are their respective exponents*.

Theorem 2.9. *Since FLT asserts* n *is even in (1), it asserts that for* $r = \prod p_i \wedge \varepsilon_i$ *and for* $s = \prod q_i \wedge \delta_i$ *there exists no exponent for either integer that is common to every prime for that intgeger.*

The example provided by FTL motivates a certain theorem on theorems following on an early paper by the author [A].

Definitions 2.10. A *context set* $\mathcal{C}$ is a set of assertions about real numbers containing n non-empty, partitionable, proper subsets $\mathcal{A}_i$, $1 < i \leq n$, such that:

Definition 2.10.1. $\mathcal{A}_i \subsetneq \mathcal{A}_{i+1}$. This is the context.

Definition 2.10.2. Iff $i = j$, then $a(\mathcal{A}_i) = c(\mathcal{A}_j)$.

Obvious examples of partitions include {negative,{0},positive} and {rational,irrational}. Directly from definitions 2.10 and the transitive nature of $\subsetneq$:

Lemma 2.11. *If* $\{X,Y\} \subset \mathcal{C}$ *such that* $\{X \cup Y\} - \{X \cap Y\}$ *is not empty, then* $\{X \cup Y\} - \{X \cap Y\}$ *is a partition of* $\mathcal{A}_j$ *and* $\{X \cap Y\} = \mathcal{A}_i$, $i < j$.

Let $a(\mathcal{A}_i)$ denote $a \in \mathcal{A}_i$.

Definition 2.12. For fixed $a(\mathcal{A}_i)$ $\exists!$ a one-to-many mapping from $a(\mathcal{A}_i)$ into $(\mathcal{A}_{i+1})$ such that $a(\mathcal{A}_i) \rightarrow c(\mathcal{A}_{i+1})$ where $\rightarrow$ denotes implication.

Note that if, and only if, $i = n$, then $\mathcal{A}_{i+1} = \mathcal{C}$. Directly from definitions 2.10.2 and 2.12, the transitive nature of implication, and the previously visited fact that the positive integers are closed under addition:

Lemma 2.13. *Iff* i = j *and* $a(\mathcal{A}_i) \rightarrow c(\mathcal{A}_j)$, *then* $a(\mathcal{A}_i) \leftrightarrow c(\mathcal{A}_j)$, *where* $\leftrightarrow$ *denotes equivalence.*

Definition 2.14. A **theorem** $T(\mathcal{C})$ on $\mathcal{C}$ is the syllogism $a(\mathcal{A}_k) \rightarrow c(\mathcal{A}_i)$, $k - i > 1$.

Definition 2.15. A **contextual** element of $T(\mathcal{C})$ is an element of the form $a(\mathcal{A}_i) \leftrightarrow c(\mathcal{A}_j)$.

Theorem 2.16. *The less the number of contextual elements in* $T(\mathcal{C})$, *the harder the theorem is to prove.*

Proof. It follows from definitions 2.10.1, 2.14 and 2.15 that each time an element of the syllogism is not contextual, one must go outside the context of $\mathcal{C}$ in order to construct a proof.

To recall the concrete example from FLT:

$\mathcal{C} =$ | $n = 2 \rightarrow n$ is even $\leftrightarrow$ equation (1) has two solutions $\rightarrow$ equation (1) has a solution.

$\mathcal{A}_1$ $\mathcal{A}_2$ $\mathcal{A}_3$ $\mathcal{A}_4$

To get from $\mathcal{A}_4$ to $\mathcal{A}_1$ in this example, one must go outside the context of $\mathcal{C}$ three times.

Definition 2.17. Let $\sum[a(\mathcal{A}_j) \rightarrow c(\mathcal{A}_i)]$ be the total number of elements in the syllogism $T(\mathcal{C})$ and let $C[a(\mathcal{A}_j) \leftrightarrow c(\mathcal{A}_i)]$ be the number that are contextual.

Directly from theorem 2.16 and definition 2.17:

Theorem 2.18. *The difficulty in proving* $T(\mathcal{C})$ *1 is monotone increasing as the ratio* $0 \leq C[a(\mathcal{A}_j) \leftrightarrow c(\mathcal{A}_i)]\{\sum[a(\mathcal{A}_j) \rightarrow c(\mathcal{A}_i)]\}^{-1} \leq 1$.

Note that in the above example based on FLT the ratio is ¾. Although $\mathcal{C}$ has a finite number of defined subsets, there can be infinitely many elements in the subsets (countable or uncountable depending upon whether they are rational or not, respectively). Based on the boundary conditions there can be a countably infinite number of rational fractions in the range $0 \leq C[a(\mathcal{A}_j) \leftrightarrow c(\mathcal{A}_i)]\{\sum[a(\mathcal{A}_j) \rightarrow c(\mathcal{A}_i)]\}^{-1}$. Hence, the chief result of the present paper.

Theorem 2.19 (chief result). *There exists infinitely many theorems as hard to prove as FLT.*

3. Conclusions

Two reasons have been formally proved to help explain why the proof of FTL was centuries in coming and turns out to be so voluminous and complex. This motivates a theorem on theorems concerning how hard a theorem is to prove. That theorem on theorems tells us there are infinitely many theorems as difficult to prove as FLT lying in wait.

References

[A] A. Allen, Measuring the Empirical Properties of Sets. IEEE Trans. Sys. Man Cyber **SMC-4**, 1974, 66-73.

[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.