FERMAT'S LAST THEOREM CAN ONLY BE RIGOROUSLY PROVED BY FIRST PROVING A SIMILAR THEOREM FOR *ALL* POSITIVE RATIONAL FRACTIONS

ALLEN D. ALLEN

ABSTRACT. The only way to prove Fermat's Last Theorem with logical rigor is to first prove Fermat's Extended Last Theorem (FELT): If n is an integer greater than 2, then there cannot exist positive rational fractions r, s, and t, neither integral nor non-integral, such that $r^n + s^n = t^n$.

1. Introduction

Pierre de Fermat had a copy of Bachet's 1621 translation of *Arithmetica* by Diophantus of Alexndria [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 what has come to be called his last theorem: "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." Since Fermat subsequently presented a proof limited to the exponents 3 and 4, it is doubtful he really had a proof for his theorem.

The proof we now enjoy, thanks to Wiles [W], is voluminous, running over 200 pages, and not merely too big for a margin. His proof is based on the Tamiyama-Shimura conjecture about modular functions of elliptic curves, following on the work of many other mathematicians [Ka, Ko, S]. Wiles' proof was first presented in 1993 but had a flaw. In 1995, the flaw was bypassed by Taylor and Wiles [F]. The proof is long and difficult. But it has now been scrutinized for 21 years and is generally accepted. But precisely what has been proved by this long, complex argument?

2. Fermat's Last Theorem

Let FLT denote Fermat's classic theorem on the Diophantine equations in N = {the positive integers} $\subset$ R = {the positive rational fractions}. Accept that FLT is true. Then a more inclusive theorem can be proved in R.

2.1 **Fermat's Extended Last Theorem (FELT)**. *There exists no integer* n *> 2 such that* $r^n + s^n = t^n$, *where* r, s, *and* t *are positive rational fractions.*

Proof. From the hypothesis that r, s, and t are positive rational fractions, it follows that

$$r = a/b, \tag{1}$$
$$s = c/d, \tag{2}$$
$$t = e/f, \tag{3}$$

where a and b are positive integers, c and d are positive integers, and e and f are positive integers. Let n be a positive integer such that

$$r^n + s^n = t^n. \tag{4}$$

Substituting from (1)-(3) into (4) we have

$$(a/b)^n + (c/d)^n = (e/f)^n. \tag{5}$$

With common denominators (5) becomes

$$[(adf)^n/(bdf)^n] + [(cbf)^n/(bdf)^n] = [(ebd)^n/(bdf)^n]. \tag{6}$$

Multiply both sides of (6) by $(bdf)^n$ to obtain

$$(adf)^n + (cbf)^n = (ebd)^n. \tag{7}$$

Since a, b, c, d, e and f are positive integers and the positive integers are closed under multiplication, it follows from (7) and FLT that $n \leq 2$.

The problem should be immediately apparent.

2.2 **Theorem**. *FTL implies FELT and FELT implies FLT.*
Proof. Consider how FELT was proved. If FLT is true, then FELT is true, as proved above. This means,

$$\text{FLT} \rightarrow \text{FELT}, \tag{8}$$

where $\rightarrow$ denotes implication. But if FLT is false, then FELT is false because it is false for the positive rational fractions that are positive integers. This means,

$$\sim\text{FLT} \rightarrow \sim\text{FELT}, \tag{9}$$

where ~ denotes negation. As is well-known, a proposition and its contrapositive are logically equivalent. Hence it follows from (9) that,

$$\sim(\sim\text{FELT}) = \text{FELT} \ \rightarrow \sim(\sim\text{FLT}) = \text{FLT}. \tag{9}$$

2.3 *Discussion*. The problem is that the elements of Diophantine FLT are in N, the elements of FELT are in R, and N is *properly* contained in R. In other words, all positive integers are positive rational fractions but the converse is not true. For, consider the proper subset $R^* \subset R$ containing all reduced rational fractions with relatively prime numerators and denominators, and the disjoint union $R' = R^* \cup N$. Every element of N is contained in R' with a denominator of one. Hence, FELT implies FLT. But no element of $R^* \subset R'$ with a denominator greater than one is in N. This means that FLT and FELT are *not* equivalent, as stated by theorem 2.2. What are we to make of this paradox? There is exactly one answer,

2.5 **Chief Result**. *No proof of FTL is logically valid unless it proves FTL by proving FELT.* This resolves the paradox because we no longer need to use FLT to prove FELT when the way FLT was proved was to prove FELT first, which then implies FLT as a corollary, as shown in (9). Indeed, to do so would be to engage in circular reasoning.

3. CONCLUSIONS

Since the only way to prove FLT is by proving FELT, Fermat's original theorem on Diophantine equations should be relegated to the history books and replaced with FELT. It is beyond the scope of this brief note to explore whether Taylor and Wiles proved FELT. But in light of the foregoing, it is a good question.

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).

[Ka] A. Knapp, *Elliptic curves*, Princeton University Press, Princeton, NJ 1992.

[Ko] N. Koblitz, *Introduction of elliptic curves and modular forms*, Springer-Verlag, Berlin, BRD, Heidelberg, BRD, New York, NY 1984.

[S] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, Berlin, Heidelberg, New York, NY 1986.

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

.

The author is retired from CytoDyn, Inc., Vancouver, WA, USA.

E-mail: allend.allen@yahoo.com

MSC 2000 Categories 03B25, 11D41