A Challenge for Undergraduate Math Majors

by

Peter Schorer

(Hewlett-Packard Laboratories, Palo Alto, CA (ret.))
2538 Milvia St.
Berkeley, CA 94704-2611
Email: peteschorer@gmail.com
Phone: (510) 548-3827

Aug. 25, 2020

Introduction

This paper is a challenge to undergraduate math majors to see if they can find an error in either of two simple approaches to a possible proof of a famous theorem, namely, Fermat's Last Theorem (FLT). All the student needs to know is the definition of congruence — a concept that is covered in any elementary number theory course at the undergraduate level.

Further details on the challenge are given below under "The Challenge" on page 3. But first I need to say a little more about FLT, its history, and one of the strategies used in this paper.

Statement of the Theorem and Brief History

Fermat's Last Theorem (FLT) states that:

For all n greater than 2, there do not exist x, y, z such that $x^n + y^n = z^n$,
where x, y, z, n, are positive integers.

It was originally stated by the French mathematician Pierre de Fermat (1601-65).

For more than 300 years, until the mid-1990s, this was the most famous unsolved problem in mathematics. No one was able to find a proof using the mathematical tools at Fermat's disposal, or using any other, far more advanced, tools either, although the attempts produced numerous results, and at least one new branch of algebra, namely, ideal theory in the 19th century.

Then in summer of 1993, a proof was announced by Princeton University mathematics professor Andrew Wiles. (Actually, Wiles announced a proof of a special case of the Shimura-Taniyama Conjecture — a special case that implies FLT.)[1] Wiles' proof was more than 100 pages long and had required more than seven years of dedicated effort. It made use of some of the most advanced mathematics of the time, and offered several new advancements of fundamental importance. A gap in the proof was discovered later that summer, but Wiles, working with Richard Taylor, was able to fill it by the end of Sept. 1994.

However, the question still remains, Does a simple proof of FLT exist? I must state immediately that the vast majority of mathematicians are convinced that the answer is No. They believe that if a simple proof exists, it would have been discovered before Wiles' proof.

One reason why I believe a simple proof might still be found is the following. Over the 300 years of attempts to find a proof, the central strategy was to expand the range of exponents for which FLT was true. Thus, Fermat claimed, in a letter to Carcavi, that he had proved the Theorem for the case $n = 4$; but he did not give full details[2]. Euler gave an incomplete proof for the case $n = 3$ in the early 18th century; Gauss gave a complete proof in the early 19th. Then, also in the early 19th century, Dirichlet and Legendre proved it for $n = 5$ and Dirichlet in 1832 proved it for $n = 14$. Lamé proved it for $n = 7$ in 1839. Kummer then proved that the Theorem was true for all "regular" prime exponents, a class of primes he defined. Among the primes less than 100, only 37, 59, and 67 are not regular. The set of n for which the Theorem was true continued to be

1. Aczel, Amir D., *Fermat's Last Theorem*, Dell Publishing, N. Y., 1996, pp. 123 - 134.
2. Kline, Morris, *Mathematical Thought from Ancient to Modern Times*, Oxford University Press, N.Y., 1972, p. 276.

expanded in succeeding years until, by the time of Wiles' proof, FLT was known to be true for all n less than 4,000,000.

We can call this strategy of expanding the size of n for which FLT is valid, the "Horizontal Approach", because for each n the goal is to prove that FLT is true for all x, y, z, here imagined as constituting a "horizontal" set relative to the "vertical" direction of progressively increasing n.

But there is another approach, one that we can call the "Vertical Approach". Here, we assume that x, y, z are elements of a counterexample to FLT, then we attempt to find the n such that $x^n + y^n = z^n$, proceeding from $n = 3$ to $n = 4$ to $n = 5$, etc., i.e., proceeding in the "vertical" direction of progressively increasing n relative to the fixed x, y, z. If we can show that we can never "get to" such an n for any x, y, z, or that the existence of such an n is impossible in the vertical sequence of cases, $(x^k + y^k, z^k)$, where $k \geq 3$, then we will have a proof of FLT.

Another way of regarding the Vertical Approach is to say that it asks what sequence of calculations would terminate in the counterexample, assuming x, y, z were known to be elements of a counterexample, and assuming the calculations were the sequence of comparisons of $x^k + y^k$ with z^k for $k = 3$, then $k = 4$, then $k = 5$, etc. This is, in fact, the form in which the Vertical Approach first occurred to me when I became interested in FLT. I was at the time writing programs, and thus immediately thought about the task of trying to find a counterexample using the computer.

Let me stop there. If you are interested in more of the reasons why I believe a simple proof of FLT might still be found, see "Why Should We Hold Out Any Hope That a 'Simple' Proof Exists?" and "Brief Summary of Approaches Described in this Paper" in Part (1) of the paper "Is There a 'Simple' Proof of Fermat's Last Theorem?" on occampress.com.

The Challenge

The Challenge is to find an error in one (or both) of the sections, "Approach Via Inner Products" on page 3, and "Approach Via the Binomial Theorem" on page 4 and to fix it. Let me know what the error is and what your fix is by writing me at the email address on the first page of this paper. Of course, if you can't find an error, I would like to know that, too! Or if you can't fix the error you find. *I guarantee that all responses I receive will be kept completely confidential. Neither the name, nor email address, nor university of the person responding will be revealed to anyone*.

You are obviously welcome to tell other students about this paper, but if a professor did not tell you about this paper originally, I must caution you about mentioning it to him or her, since he or she will almost certainly regard it as the work of a crackpot (which I am not — my degree is in Computer Science and the main part of my career has been as a researcher in the computer industry). He or she might very well regard you as less-than-bright for spending any time on such a paper, since "everyone" in the mathematics community knows there is no simple proof of FLT.

Approach Via Inner Products

Assume a counterexample $x^p + y^p = z^p$ exists, where p is prime and is the smallest such p.

We can write the equation as $x^p + y^p - z^p = 0$, and then express it as an inner product equation $\langle (x^{p-1}, y^{p-1}, z^{p-1}), (x, y, -z) \rangle = 0$. (We can also express it as $\langle (x^{p-k}, y^{p-k}, z^{p-k}), (x^k, y^k, -z^k) \rangle = 0$, where $1 \leq k \leq p - 1$.)

Now x^{p-1} has one and only one value, whether or not a counterexample exists. Similarly for

y^{p-1}, z^{p-1}, x, y, and $-z$. But then the inner product must be exactly the same whether or not a counterexample exists — that is, $x^p + y^p - z^p = 0$ whether or not a counterexample exists. This is a contradiction. If our reasoning is correct, we have a proof of FLT.

Remark: A reader has written us stating that our argument is invalid, because it is known that if x, y, z are non-positive-integer real numbers, then counterexamples exist, and our argument applies in that case, hence is false. However, this criticism is invalid: FLT applies only to positive integers, and that is what our argument applies to. Far more important is the fact that a proof must stand or fall on its own, and it is incumbent upon us to ask: suppose one did not know about the existence of counterexamples if x, y, z are non-positive-integer reals. What would then be the criticism that our argument is invalid?

Approach Via the Binomial Theorem

This Approach is from the section, "First Approach Via the Binomial Theorem," Part (1) of the paper "Is There a 'Simple' Proof of Fermat's Last Theorem?" on occampress.com.

1. Let x, y, z, p be constituents of the minimal counterexample. Now let us find the difference between $(x^p + y^p - z^p)$ and $((x-1)^p + (y-1)^p - (z-1)^p)$. That is, let us find

(1)
$$(x^p + y^p - z^p) - ((x-1)^p + (y-1)^p - (z-1)^p).$$

2. For $v = x$ or y or z, let

$U(v, p) = E(v-1)^p - v^p$, where E denotes the binomial expansion of $(v-1)^p$, (Clearly the binomial expansion, $E(v-1)^p$, of $(v-1)^p = (v-1)^p$.) Thus we have $v^p + U(v, p) = E(v-1)^p$, and:

$$x^p + U(x, p) = E(x-1)^p;$$
$$y^p + U(y, p) = E(y-1)^p;$$
$$z^p + U(z, p) = E(z-1)^p.$$

Then (1) becomes

(2)
$$(x^p + y^p - z^p) - ((x^p + U(x, p)) + (y^p + U(y, p)) - (z^p + U(z,p)))$$

3. But since $(x^p + y^p - z^p) = 0$, and since $-x^p - y^p + z^p$ is simply the negative of $(x^p + y^p - z^p)$ which = 0, we get, from (2)

(3)
$$-U(x, p) - U(y, p) + U(z,p).$$

4. Now assume instead that x, y, z, p are *not* the constituents of a counterexample, in other words assume that a counterexample does not exist.

But the value of the difference in (1), as expressed by (3), is exactly the same, because now x^p in $(x^p + y^p - z^p)$ and $- x^p$ in the right-hand part of (2), cancel, and similarly for y^p and $- y^p$, and z^p and $- z^p$.

5. So we must conclude that there is no difference between the value of $(x^p + y^p - z^p)$ if it is a counterexample and if it is not.

This contradiction arose from our assuming that a counterexample exists. Therefore, if our reasoning is correct, a counterexample does not exist, and we have a proof of FLT.