

# **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@cs.com](mailto:peteschorer@cs.com)

Phone: (510) 548-3827

Apr. 28, 2011

## Introduction

This paper is a challenge to undergraduate math majors to see if they can find an error in a very simple approach 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 the Strategy 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.)<sup>1</sup> 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.

But 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<sup>2</sup>. 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 1980s, it consisted of all odd primes less than 125,000. (It can easily be shown that this implies the Theorem was true for all exponents, prime or composite, less than 125,000.)

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, since this is all you need in order to understand the Strategy in the Challenge. The Strategy is an example of the Vertical Approach. 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](http://occampress.com).

## **The Challenge**

The Challenge is to find an error in the section, “A Possible Strategy for a Simple Proof of FLT” on page 6, and 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! *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 I was for several years a researcher at Hewlett-Packard’s main research laboratory in Palo Alto, CA). It is probably safe to approach your professor by saying, for example, words to the effect, “Excuse me, Prof. —, but I came across this paper on the Internet and discovered an error in it.” Of course, if you are able to say that you fixed it, you should add that. If you were unable to find an error, then you can say words to the effect, “I have so far been unable to find an error in the paper. I thought I would ask you if you can.”

Now for some preliminaries.

## Fermat's Little Theorem

Central to our Strategy is a Theorem that Fermat himself stated. It is:

If  $q$  is a prime then  $a^q \equiv a \pmod{q}$ , where  $a$  is an integer.

## Definitions

### Definition of “ $U(k, a, b, c)$ ”

Let  $k, a, b, c$  be positive integers. Then  $U(k, a, b, c) = a^k + b^k - c^k$ .

### Definition of **D-set**

Let  $q$  be a prime modulus. Then a **D-set** mod  $q$ ,  $\mathbf{D}_{u, v, w, j, q}$  is defined as:

$\mathbf{D}_{u, v, w, j, q} = \{a^r + b^r - c^r = U(r, a, b, c) \mid a, b, c \equiv u, v, w \pmod{q}, \text{ respectively, where } u, v, w \text{ are the minimum residues of congruence classes mod } q, r \equiv j \pmod{q-1}; \text{ where } j \text{ is an element of } \{1, 2, 3, \dots, q-1\}, \text{ so that, by Fermat's Little Theorem, } a^r \equiv u^j, b^r \equiv v^j, c^r \equiv w^j \pmod{q}\}$ .

In each **D-set** mod  $q$ , all  $U(r, a, b, c)$  are congruent mod  $q$ . (Because  $a^r \equiv u^j, b^r \equiv v^j, c^r \equiv w^j \pmod{q}$  and  $U(r, a, b, c) = a^r + b^r - c^r$ .) Hence each **D-set** constitutes elements of a congruence class mod  $q$ , and there is always an infinity of elements in each **D-set**, since there is always an infinity of  $r \equiv j \pmod{q-1}$  for each  $j$ .

### Definition of Fixed-set **F**

We begin with some examples.

We cannot seriously imagine a professional mathematician saying, prior to Wiles' proof of FLT, things like, “Well, of course we know that  $17^7 + 18^7 \neq 19^7$ , (because  $17^7 + 18^7 - 19^7 = 128,686,966$ , not 0), but if a counterexample is proved to exist, then this might change. That is,  $17^7 + 18^7 - 19^7$  might no longer equal 128,686,966.”

Thus, we say that  $17^7 + 18^7 - 19^7 = U(7, 17, 18, 19)$  is an element of the *fixed-set*  $F$ , because the value of  $17^7 + 18^7 - 19^7$  is fixed, regardless whether a counterexample exists or not.

Prior to Wiles' proof, namely, in the early 90s, FLT had been proved for all prime exponents (and hence for all exponents) less than 125,000. In any case, the fixed-set  $F$  includes all  $U(r, a, b, c)$  such that  $r < p$ , where  $p$  is the assumed (prime) exponent in the minimum counterexample. (If a counterexample exists, then one exists having a prime exponent.) In particular, it includes all  $U(r, x, y, z)$ , where  $r < p$  and  $x, y, z$  are the elements of the minimum counterexample.

From these initial observations, we assert that we can partition the set of all  $U(k, a, b, c)$  in all **D-sets** into two sets:

- (1) the set  $F = \{U(k, a, b, c) \mid a^k + b^k - c^k \text{ is the same regardless whether a counterexample exists or not (for this reason, we call } F \text{ the fixed set)}\}$ ,
- (2) the set  $\sim F$ , the complement of  $F$ .

To show that our definition of the set  $F$  is meaningful, we ask if, prior to Wiles' proof, it was legitimate to say, “for all  $k \geq p$ ,  $U(k, a, b, c)$  will have the same value if FLT is proved true as it will have if a counterexample to FLT is discovered (or if FLT is proved false)”.

The answer is “No, it was not legitimate! Because if a counterexample was discovered (or FLT was proved false), then some  $U(k, a, b, c)$  — namely the  $U(k, a, b, c) = U(p, x, y, z) = 0$  — would have a different value than it would have if no counterexample existed (in which case, for all  $k, a, b, c, U(k, a, b, c) \neq 0$ ).”

If we can show that the existence of a counterexample implies that some members of  $F$  are in  $\sim F$ , then that contradiction would give us a proof of FLT.

An example of an element of  $\sim F$  is, of course, the counterexample itself. If  $x^p + y^p = z^p$ , then  $x^p + y^p - z^p = U(p, x, y, z) = 0$ . But if no counterexample exists, then,  $x^p + y^p \neq z^p$ , so  $x^p + y^p - z^p = U(p, x, y, z) \neq 0$ .

### **Some Other Elements of the Fixed-set $F$**

Clearly, all  $U(r, x, y, z)$ , where  $r < p$ , are elements of  $F$ . But there are elements of  $F$  for which  $r$  in  $U(r, a, b, c) > p$ . In fact we can state the following:

All elements (an infinity of them) of each **D**-set mod  $q$  such that the minimal elements of the congruence classes in the **D**-set are  $u^j, v^j$ , and  $w^j$ , with  $j < p$ , are in the fixed-set  $F$ .

Clearly, there will be an infinity of  $U(r, a, b, c)$ , where  $r > p$ , in each such **D**-set. The reason is that there is an infinity of  $r \equiv j \pmod{q-1}$  for each  $j$ . All the  $U(r, a, b, c)$  in each such **D**-set are in the fixed-set  $F$ , because  $U(j, u, v, w)$  is. That is, whether or not a counterexample exists, each  $U(j, u, v, w)$  has one, fixed value. Therefore, whether or not a counterexample exists, each of the following has one, fixed value:

$$\begin{aligned} &U(j, u, v, w), \\ &U(j, u, v, w) + 1q, \\ &U(j, u, v, w) + 2q, \\ &U(j, u, v, w) + 3q, \\ &U(j, u, v, w) + 4q, \end{aligned}$$

...

Since each  $U(r, a, b, c)$  in each such **D**-set is one of the values in this infinite list, each such  $U(r, a, b, c)$  has one, fixed value whether or not a counterexample exists, and hence is in the fixed-set  $F$ .

Note that if the values of all  $U(r, a, b, c)$  except  $U(p, x, y, z)$  were each chosen at random, then the fixed set  $F$  would contain *all*  $U(r, a, b, c)$  *except*  $U(p, x, y, z)$ .

### **Some Other Elements of $\sim F$**

Let  $x^p + y^p = y^p$  be a counterexample to FLT, and let  $q$  be a prime modulus such that  $x^p = u^p, y^p = v^p, z^p = w^p$  are the minimum residues for a **D**-set mod  $q$ . Since  $U(p, x, y, z) = 0$ , all  $U(r, a, b, c)$  in the **D**-set are congruent to 0 mod  $q$  and therefore are multiples of  $q$ . There is an infinity of such  $q$ . But if  $x^p + y^p \neq y^p$ ,  $U(p, x, y, z) = 0$  for only a finite number of moduli  $q$ , namely, the  $q$  that are prime factors of  $U(p, x, y, z)$ . So for an infinite number of moduli  $q$ , namely, all  $q$  that are not fac-

tors of the  $U(p, x, y, z)$ , the  $U(r, a, b, c)$  of the **D**-set mod  $q$  containing  $U(p, x, y, z)$  are not multiples of  $q$ . So the elements of an infinite number of **D**-sets are in  $\sim F$ .

## **A Possible Strategy for a Simple Proof of FLT**

### **First Implementation**

Consider the prime modulus  $q = 2$ . Since  $q - 1 = 1$ , there is a **D**-set mod 2 containing the following  $U$  terms:

$$U(1, x, y, z),$$

$$U(2, x, y, z),$$

$$U(3, x, y, z),$$

....

By what we have said in the section “Definition of D-set” on page 4, all the elements of this **D**-set are in the fixed-set  $F$ . But one of these elements is  $U(p, x, y, z)$ , which obviously cannot be in the fixed-set unless it is not the element for a counterexample! This contradiction gives us our proof of FLT.

### **Second Implementation**

By basic algebra, it is easy to show that

$$(1) \quad (x^{p-1} + y^{p-1} - z^{p-1})(x + y + z) + g(x, y, z) = x^p + y^p - z^p,$$

where  $g(x, y, z)$  is an algebraic expression involving products of powers of  $x, y, z$ . It follows that:

$$(2) \quad x^{p-1} + y^{p-1} - z^{p-1} = (x^p + y^p - z^p - g(x, y, z))/(x + y + z).$$

Clearly  $x^{p-1} + y^{p-1} - z^{p-1} = U((p-1), x, y, z)$  is a member of the fixed set  $F$ . But if  $x^p + y^p - z^p$  is a counterexample,  $U((p-1), x, y, z)$  will have a different value than if  $x^p + y^p - z^p$  is not a counterexample. Thus a member of the fixed set is a member of its complement, a contradiction. And thus FLT is proved.

Another way of stating this conclusion is that we have shown that, since  $U((p-1), x, y, z)$  is a member of the fixed set  $F$ , a counterexample has the same value as a non-counterexample, or, informally, that all counterexamples are non-counterexamples, one interpretation of which is that the set of counterexamples is the null set.

## **The Concept at the Heart of This Strategy**

The heart of our Strategy is the fact that a counterexample “has consequences”. The briefest explanation I can give of what this means is the following: let  $S$  be a 4-dimensional space in which each point is a 4-dimensional cube, with all cubes being the same size. The cube having coordinates  $(r, a, b, c)$  contains  $U(r, a, b, c)$ . It should be immediately clear that if  $c$  is a cube, then

the value in each adjacent cube is related to the value of  $c$ , where an *adjacent cube* is one in which just one coordinate differs from the corresponding coordinate of  $c$ . In fact, we can compute the value of the adjacent cube *from* the value in  $c$ . So if the value in  $c$  is 0 (which would be the case if a counterexample to FLT existed), then the values in adjacent cubes will differ from what they would be if the value in  $c$  were not 0. This is what I mean when I say that a counterexample “has consequences”.

As I said in the section, “Some Other Elements of the Fixed-set F” on page 5, if the value of each  $U(r, a, b, c)$  were chosen at random, then a counterexample would *not* have consequences, because the value in each cube adjacent to a cube  $c$  that contained 0, would have no relationship to 0. We could not determine this value *from* the value 0.

For further details, see the section “‘Consequences’ of a Counterexample” in Part (4) of “Is There a ‘Simple’ Proof of Fermat’s Last Theorem?” on [occampress.com](http://occampress.com), and also the section “Four-Dimensional Approach” in Part (1) of the same paper. This latter section discusses the possibility of “crooked induction” from the cube that contains an assumed counterexample.