Is There a "Simple" Proof of Fermat's Last Theorem?

Part (1)
Introduction and Several New Approaches

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. 7, 2024

Abstract

We present several approaches to a possible "simple" proof of Fermat's Last Theorem (FLT), which 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. Until the mid-1990s, when a proof was given by Andrew Wiles, this had been the most famous unsolved problem in mathematics. But Wiles' proof was well over 100 pages long, and involved some of the most advanced mathematics of its time, and so the question lingers, "Is there a 'simple' proof of the Theorem?"

Note 1:
Without question, our best Approaches to a simple proof of FLT are:

"Approach Using Basic Algebra" on page 31 of this Part (less than one page).
"Approach Using 'Neighborhood' of Assumed Counterexample" on page 32 of this Part (less than one page).
"Four-Dimensional Cartesian Grid Approach" on page 35 of this Part (less than a page).
''Approach Using Pythagorean Theorem" on page 33 of this Part (less than one page)
"Approach Using Inner Products" on page 32 of this Part (less than two pages);

Note 2: We are seeking a prolific published number theorist to help us prepare one or more proofs based on the above Approaches (or others in this paper) for submission to an appropriate journal. We will offer a generous consulting fee, and, if the paper is published, generous credit in the Acknowledgments, which will result in considerable prestige for the number theorist.

Part (2) of this paper contains proofs of lemmas not proved in this Part;
Part (3) contains descriptions of failed implementations of some ideas in this Part;
Part (4) contains several possible proofs involving the "lines and circles" model of congruence.

All Parts are on occampress.com.

Key words: Fermat's Last Theorem

Statement of the Theorem and Brief History

Fermat's Last Theorem (FLT) states:

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.

Until the mid-1990s, this was the most famous unsolved problem in mathematics. It was originally stated by the 17th century mathematician Pierre de Fermat (1601-65).

"In about 1637, he annotated his copy (now lost[1]) of Bachet's translation of Diophantus' *Arithmetika* with the following statement:

> Cubem autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere: cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caparet.

"In English, and using modern terminology, the paragraph above reads as:

> There are no positive integers such that $x^n + y^n = z^n$ for n greater than 2 . I've found a remarkable proof of this fact, but there is not enough space in the margin [of the book] to write it."

— Dept. of Mathematics, University of North Carolina at Charlotte
(http://www.math.uncc.edu/flt.php)

For more than 300 years, 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. 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.)[2] Wiles' proof was 200 pages long and had required more than seven years of dedicated effort. 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.

Did Fermat Prove His Theorem?

Arguments That Fermat Didn't Prove His Theorem

It is safe to say that virtually all professional mathematicians believe that the answer to this question is no. For example:

"Did Fermat prove this theorem?

"No he did not. Fermat claimed to have found a proof of the theorem at an early stage in his career. Much later he spent time and effort proving the cases $n = 4$ and $n = 5$. Had he had a proof

[1] An obvious question is, If the original copy is lost, how do we know what his note said? Apparently his son, during the course of going through Fermat's papers after his death, found the copy of Bachet's translation and, in leafing through it, saw Fermat's note and copied it down.

[2] Aczel, Amir D., *Fermat's Last Theorem*, Dell Publishing, N. Y., 1996, pp. 123 - 134.

to his theorem, there would have been no need for him to study specific cases.

"Fermat may have had one of the following "proofs'" in mind when he wrote his famous comment.

"Fermat discovered and applied the method of infinite descent, which, in particular can be used to prove FLT for $n = 4$. This method can actually be used to prove a stronger statement than FLT for $n = 4$, viz, $x^4 + y^4 = z^2$ has no non-trivial integer solutions. It is possible and even likely that he had an incorrect proof of FLT using this method when he wrote the famous theorem".

"He had a wrong proof in mind. The following proof, proposed first by Lamé was thought to be correct, until Liouville pointed out the flaw, and by Kummer which latter became and [sic] expert in the field. It is based on the incorrect assumption that prime decomposition is unique in all domains.

"The incorrect proof goes something like this:

"We only need to consider prime exponents (this is true). So consider $x^p + y^p = z^p$. Let r be a primitive p-th root of unity (complex number).

"Then the equation is the same as:

"$(x + y)(x + ry)(x + r^2y)...(x + r^{(p - 1)}y) = z^p$

"Now consider the ring of the form:

"$a_1 + a_2\, r + a_3\, r^2 + ... + a_{(p - 1)}\, r^{(p - 1)}$

"where each a_i is an integer.

"Now if this ring is a unique factorization ring (UFR), then it is true that each of the above factors is relatively prime. From this it can be proven that each factor is a pth power and from this FLT follows.

"The problem is that the above ring is not an UFR in general.

"Another argument for the belief that Fermat had no proof — and, furthermore, that he knew that he had no proof — is that the only place he ever mentioned the result was in that marginal comment in Bachet's Diophantus. If he really thought he had a proof, he would have announced the result publicly, or challenged some English mathematician to prove it. It is likely that he found the flaw in his own proof before he had a chance to announce the result, and never bothered to erase the marginal comment because it never occurred to him that anyone would see it there.

"Some other famous mathematicians have speculated on this question. Andre Weil, writes:

"'Only on one ill-fated occasion did Fermat ever mention a curve of higher genus $x^n + y^n = z^n$, and then[sic] hardly remain any doubt that this was due to some misapprehension on his part [for a brief moment perhaps] [he must have deluded himself into thinking he had the principle of a general proof.]'

"Winfried Scharlau and Hans Opolka report:

"'Whether Fermat knew a proof or not has been the subject of many speculations. The truth seems obvious ...[Fermat's marginal note] was made at the time of his first letters concerning number theory [1637]...as far as we know he never repeated his general remark, but repeatedly made the statement for the cases $n = 3$ and 4 and posed these cases as problems to his correspondents [he formulated the case $n = 3$ in a letter to Carcavi in 1659 [All these facts indicate that Fermat quickly became aware of the incompleteness of the [general] "proof" of 1637. Of course, there was no reason for a public retraction of his privately made conjecture.'

"However it is important to keep in mind that Fermat's 'proof' predates the Publish or Perish period of scientific research in which we are still living."

— Dept. of Mathematics, University of North Carolina at Charlotte, (http://www.math.uncc.edu/flt.php) Jan. 31, 2004 (brackets (except in "[sic]"s) and quotation marks as in the original as they appeared on our computer screen)

A Very Cautious Speculation That Perhaps Fermat Did Prove His Theorem

Despite the above skepticism, we believe that some of the approaches to a proof of FLT that are set forth in this paper might have been within reach of Fermat. But we hasten to state clearly and unequivocally that **we make no claims of a proof** in this paper, or anywhere else in our writings.

All the attempts that we are aware of to prove FLT prior to Wiles' proof in the mid-1990s have been centered on expanding the range of exponents n for which FLT is true. As we state in "Why Should We Hold Out Any Hope That a "Simple" Proof Exists?" on page 6:

"We can call this strategy 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 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, then we will have a proof of FLT." Vertical Approaches are described in Part (4) of this paper, on occampress.com.

When Did Fermat Make the Note in the Margin?

Mathematicians who are normally cautious to a fault about making statements even with all the material before them that they need in order to prove the validity of their statements, seem to become gifted with apodictic insight when discussing the history of Fermat's efforts to prove his theorem, even though much evidence is missing and almost certainly will never be found.

Nevertheless, contrary to the standard view, it seems entirely possible that Fermat got the idea of his theorem in 1637 while reading Bachet's translation of Diophantus, made *no note* in the margin at that time but instead set out to prove the theorem as described in the above-cited letters. Then, late in life — after 1659 — possibly while re-reading Bachet, he suddenly thought of his proof, and made a note of its discovery in the nearest place to hand, namely, the margin of the book.

Why Should We Hold Out Any Hope That a "Simple" Proof Exists?

We are well aware that the vast majority of mathematicians believe that no simple proof of FLT exists. The reasoning is that, if a simple proof exists, it would have been discovered before Wiles' proof. So the reader is perfectly justified in asking, "Why bother spending even five minutes more on the question of a 'simple' proof?" We think there are several reasons:

• Most of the research on FLT over the more than three centuries prior to Wiles' proof centered on expanding the size of the exponent n for which FLT is true. We call this strategy 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 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 assumption that for some n, $x^n + y^n = z^n$ leads to a contradiction, then we will have a proof of FLT. More details are given under ""Vertical" Approaches" on page 10.

• The computer has pushed the deductive horizon far beyond that of even the best mathematicians of the past, where by "deductive horizon" we mean the limit of mathematicians' ability to carry out long deductions. For example, we believe that in the near future, it will be possible to input to a computer program all the theorems and lemmas and rules of deduction that scholars have reason to believe that Fermat had at his disposal at the time he made the famous note in the margin of his copy of Diophantus, and to ask the program to find a proof of FLT. For a further discussion, see "Can We Find Out If Fermat Was Right After All?" on page 59.

• New conceptual machinery is constantly appearing that might make a simple proof possible. We are thinking specifically of computation theory. An attempt to use some of this machinery is given in the section ""Computational" Approaches" on page 59.

• We don't know all the approaches that have been tried in the past, since the mathematics community records only the (published) successes, however partial, that were achieved in the long years of attempting to prove the Theorem. Furthermore, from the beginning of the 19th century, if not earlier, the professionalization of mathematics tended to result in the relegation of the work of amateurs to the crackpot category. (And yet Fermat, Pascal, Descartes, Leibniz and many other leading mathematicians (as well as many physicists) of the 17th century were amateurs!)

We were told by several professional mathematicians prior to Wiles' proof, that whenever an envelope arrived containing a manuscript with "Fermat's Last Theorem" in the title, and the manuscript was by an author who was not a tenured professor, the manuscript went unread straight into the wastebasket. Such a practice was, we now know, justified in the past regarding claims of solutions to the three classic unsolved problems of the Greeks — squaring the circle, doubling the cube, and trisecting the angle, each to be done using only straightedge and compass — because, as was proved in the 19th century, solutions to these problems, under the constraint of using only straightedge and compass, do not exist. But FLT is different, in that we now know that it is true. No doubt all, or very nearly all, of the manuscripts that mathematicians received from amateurs were, in fact, flawed, if not outright crackpot, works. Furthermore, overworked professional mathematicians have a perfect right to spend their time on the material they think it worth spending their time on. Nevertheless, it is possible, however unlikely, that one of the amateurs' manuscripts, even if it contained errors, also contained the germ of an idea that might have led to a "simple" proof of FLT. We will never know. In any case, if a record of amateurs' attempts had been maintained by the mathematics community — if only for the derisive amusement of professional mathematicians — this might have saved many amateurs from endlessly repeating some of the doomed efforts of their predecessors.

We must say that we are not ashamed to admit that for us, the study of amateurs' efforts to solve very difficult problems has a certain psychological interest. Fundamentally, it seems to us, the study is no different from the study of primitive tribes' attempts to explain the universe. In any case, we believe in the possibility of "brilliant failures".

But we fully recognize that no professional mathematician considers such a study to be worth even mentioning.

• "Wiles' proof used some mathematics that depends on the Axiom of Choice. But there is a theorem that any theorem of number theory that uses the Axiom of Choice has a proof that doesn't. So, somewhere, there is a simpler, or at least less high-powered, proof of Fermat." — email from Michael O'Neill.

• Finally, it is possible (however unlikely) that certain approaches to a possible solution were discarded time and again, even by amateurs, on the grounds that if a proof were that simple someone would have already published it.

How to Read This Paper

We are well aware that most readers will not want to read all of this paper. We therefore recommend the following: read the first nine pages, and then choose from the referenced sections under "Most Promising Approaches to a Simple Proof of FLT, in Our Opinion: Previous List" on page 11, and/or use the titles and subtitles on the left of the screen to find the topics of most interest.

The reader should keep in mind that this paper is a work-in-progress. Thus it presents not merely results, but also conjectures, discussions of approaches and of obstacles presented by various approaches. The paper is divided into four parts.

Part (1) overview of our approaches;
Part (2) statements and proofs of all lemmas;
Part (3) failed attempts to prove FLT using some of the ideas in the paper;
Part (4) details on the approach based on the "lines-and-circles" model of congruence and in particular, on the important function $U(k, a, b, c) = a^k + b^k - c^k$.

All parts are in the Fermat's Last Theorem section of our web site, www.occampress.com.

Proofs of lemmas have *not* been optimized, though virtually all of them have been checked and deemed correct by qualified readers. We have made a serious attempt to write in an accepted style, but the organization of the four parts of the paper certainly does not always follow that of a published paper. Lemma numbering is not always consecutive because we want to preserve the numbering in earlier versions of the paper, even though new lemmas have been added.

References to definitions, lemmas, and proofs are usually given with section title, part of the paper, and usually the page number. The .pdf file format provides a list of titles and sub-titles on the left-hand side of the text, which should make it relatively easy for the reader to navigate through each part of the paper.

Why Is It So Difficult to Prove FLT?

Our question should read in full, "Why is it so difficult to prove FLT at the elementary level represented by the approaches in this paper?" We believe there are two main reasons:

Two Main Reasons

(1) We (meaning, here, the author of this paper) simply do not know all the results in the FLT literature that might enable us to make progress in approaches to a proof at the elementary level.

(2) "Local" approaches do not seem to work. An example of what we mean by a "local" approach is a proof by contradiction in which we consider only the assumed counterexample $x^p + y^p = z^p$, and do not consider, for example, the pairs $\{x^{p-k} + y^{p-k}, z^{p-k}\}$, The approaches referenced under "Most Promising Approaches to a Simple Proof of FLT, in Our Opinion: Previous List" on page 11 are all "global".

We believe that one valuable outcome of research into the possibility of a proof of FLT by elementary means, would be the determining, in far more detail than we have done here and in the next section, one or more guidelines for avoiding the fruitless labors that we are sure have consumed so much time among researchers who have attempted to prove FLT using elementary means. (Virtually all of these researchers have been amateurs, it is safe to assume.) Such guidelines , we would hope, could be applied to other very difficult problems. Perhaps the research will reveal that there can be no general guidelines, other than trivial ones, for avoiding fruitless labors. That result in itself would constitute progress.

A related valuable outcome of this research might be insights into ways of recognizing what I will call "prickly" problems. The term does *not* merely refer to problems that are very difficult, but rather to problems having the property that solutions are "isolated"; very few roads lead to solutions, and yet solutions exist. Among the questions we can ask is, "What are the characteristics of a formal grammar (for example, one representing the domain of the problem) such that certain strings produced by the grammar are extremely hard to find — or in other words, such that very few sequences of productions in the grammar terminate in the strings. How exactly would that be possible?"

The Danger of "Null" Approaches

A "Null" Approach is one that, although it contains the constituents x^p, y^p and z^p of an assumed counterexample, would yield the same results if x^p, y^p and z^p were replaced by any positive integers u, v, w, such that $u + v = w$. Perhaps the simplest example of a Null Approach is that of trying to derive a contradiction by multiplying the polynomial $(x + y - z)$ and the polynomial $(x^{p-1} + y^{p-1} + z^{p-1})$ and then deleting x^p, y^p and $-z^p$ from the resulting terms (see "Approaches of Multiplying Integer Polynomials" on page 37). We find, on examining what remains after the deletion, that all we have proved is that $x^p + y^p - z^p = 0$. A similar danger lurks in approaches based on the fact that, if $x^p + y^p = z^p$ then $x^p + y^p \equiv z^p \bmod m$. Since this fact is true for all moduli m, it is certainly true for each m that is an appropriate modulus, that is, for each m such that $(x, m) = (y, m) = (z, m) = 1$. The latter congruence in turn gives rise to an infinity of congruences by basic rules governing congruences. But it is true for all a, b, c that if $a + b = c$ then $a + b \equiv c \bmod m$ for any modulus m, and it is equally true that the latter congruence gives rise to an infinity of congruences.

Examples of approaches that would yield the same inconclusive results if the odd prime exponent p were replaced by any positive real k in the appropriate range, are described under ("Approaches Using the Calculus" on page 52.

At present, we believe that a good way to avoid Null Approaches is to concentrate, not merely on the assumed counterexample, but on expressions that lie "near" to the assumed counterexample, for example, to investigate what would have to be the case in order for $x^p + y^p - z^p = 0$, given that $x^{p-1} + y^{p-1} - z^{p-1} \neq 0$. This approach is developed in "Approach Via Fixed-Set" in Part (4) of this paper, on occampress.com. Another good way to avoid Null Approaches is always to see what would happen to the Approach if there were no counterexample.

The Problem of Too-Little Information

As the reader will see in going through this paper, attempts at proofs of FLT are again and again blocked by our simply having too little information about the elements x, y, z and p of an assumed counterexample, and about terms derived from these elements. In particular, this problem usually thwarts all proof attempts that rely on inequalities. At least some of the information may exist in the literature, but we are at present unaware of it.

Brief Summary of Approaches Described in This Paper

The approaches to a proof of FLT that are described in this paper are as follows:

- "Vertical" Approaches
  (see brief introduction under ""Vertical" Approaches" on page 10)

  The following Approaches are, in our opinion, the most promising.

  "Approach Using Basic Algebra" on page 31 of this Part (less than one page).
  "Approach Using 'Neighborhood' of Assumed Counterexample" on page 32 of this Part (less than one page).
  "Four-Dimensional Cartesian Grid Approach" on page 35 of this Part (less than a page).
  ''Approach Using Pythagorean Theorem" on page 33 of this Part (less than one page)
  "Approach Using Inner Products" on page 32 of this Part (less than two pages);

  Other Approaches are:

  - Vertical Approach Based on the Function $U(k, a, b, c) = a^k + b^k - c^k$
    (see "Third Promising Approach to a Simple Proof of FLT", in Appendix A of Part (4) of this paper, on occampress.com)

- Vertical Approaches Based on Binomial Theorem
  (see "First Approach Via the Binomial Theorem" on page 19,
  "Second Approach Via the Binomial Theorem" on page 20)

- Approach Involving Comparing Counterexamples and Non-Counterexamples
  (see "Approach Involving Comparing Counterexamples and Non-Counterexamples" on page 34)

- Vertical Approaches Based on Congruences
  (see "Vertical Approaches Based on Congruences" on page 21)

- Vertical Approaches by Induction on Inequalities
  (see "Vertical Approaches by Induction on Inequalities" on page 26)

- Vertical Approach Using the Calculus
  (see "Approaches Using the Calculus" on page 52)

- Vertical Approach Comparing Counterexamples and Non-Counterexamples
  (the Fixed-Set)
  (see "Approach Involving Comparing Counterexamples and Non-Counterexamples" on page 34)

- Approach Via Factors of x, y, z
  (see "Approach via Factors of x, y, z" on page 54)

- Approach Using $x = z - h$, $y = z - k$
  (see "Approach Using x = z - h, y = z - k" on page 56)

- Approaches Involving Multiplying Polynomials
  (see "Approach of Multiplying Fractional Polynomials" on page 35.
  "Approaches of Multiplying Integer Polynomials" on page 37)

- "Computational" Approaches
  (see ""Computational" Approaches" on page 59)

- *n*-Dimensional Geometric Approaches
  (see "n-Dimensional Geometric Approaches" on page 62)

"Vertical" Approaches

The "Vertical" approaches are motivated by the question, "If a counterexample existed, how would we 'get there'?" The meaning of this question will become clearer if we consider briefly the strategy that was pursued throughout most of the history of attempts to prove FLT, namely, the strategy of progressively expanding the set of exponents n for which FLT was true. (The fact that FLT was true for each of these n meant that it was true for all multiples of these n, since if $x^n + y^n \neq z^n$ for all x, y, z, then certainly $(u^k)^n + (v^k)^n \neq (w^k)^n$, for all u, v, w, $k \geq 1$.) 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[1]. 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 expanded in succeeding years until, by the 1980s, it consisted of all odd primes less than 125,000. By 1993, the Theorem was known to be true for all n up to 4,000,000.

We will 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 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, 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 $x^n + y^n$ with z^n for $n = 3$, then $n = 4$, then $n = 5$, etc. This is, in fact, the form in which the Vertical Approach first occurred to us when we became interested in FLT. We were at the time working as a programmer, and thus immediately thought about the task of trying to find a counterexample using the computer.

The skeptical reader should keep in mind that if the initial inequalities, followed by the equality that is the assumed counterexample, were unrelated to each other, then the Vertical Approach would have little to recommend it. But the inequalities, and the subsequent assumed equality, are *not* unrelated: For one thing, they all involve the same three numbers, x, y, z; for another the numbers are all raised to the same power in each inequality or in the equality; and for another they are related as described under " 'Consequences' of a Counterexample" in Part (4) of this paper, on the web site www.occampress.com.

Most Promising Approaches to a Simple Proof of FLT, in Our Opinion: Previous List

The following is a list of the approaches that at present we deem most promising. The most promising is listed first, the next-most-promising second, etc.

"Approach Using Pythagorean Theorem" on page 33;

"Approach Using Basic Algebra" on page 31 of this Part (less than one page).

"Approach Using "Neighbor" of Assumed Counterexample" on page 32

"Approach Using Inner Products" on page 32;

"Four-Dimensional Cartesian Grid Approach" on page 35 of this file;

"First Approach Via the Binomial Theorem" on page 19 of this file;

"Third Promising Approach to a Simple Proof of FLT", in Appendix A of Part (4) of this

[1] Kline, Morris, *Mathematical Thought from Ancient to Modern Times*, Oxford University Press, N.Y., 1972, p. 276.

paper, on occampress.com;

"Approach by a Certain Class of Program" on page 60 of this file;

"Third Approach of Multiplying Integer Polynomials" on page 39 of this file;

"First Implementation of Approach" on page 42 of this file (namely, of the Approach of Adding Inequalities);

Part (E) of "Approach Type IV: Considering All Multiples of All Powers of a, b, c" in Part (4) of this paper, on occampress.com.

We will offer shared authorship to the first person who helps us make any one of the above approaches, or any other approach in this paper, yield a publishable paper. *Note: before submitting improvements to the above approaches, the prospective co-author must query the author as to the status of the offer. We will not offer shared authorship without this preliminary query.*

Initial Assumptions, Definitions, and Properties of Numbers Involved

We are trying to prove Fermat's Last Theorem (FLT), which 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.

We will usually attempt a proof by contradiction. That is, we will assume there exist positive integers x, y, z such that for some n greater than 2,

(1) $x^n + y^n = z^n$.

Without loss of generality, we assume that x, y, z are relatively prime in pairs, i.e., that

(1.5) $(x, y) = (y, z) = (x, z) = 1$.

(2.0) Clearly, exactly one of x, y, z must be even.

(3.0) $x < y < z$;

(4.0) x, y, z must be very large numbers[1].

(5.0) By 1993, prior to Wiles's proof, FLT was known to be true for all exponents up to 4,000,000.

(1.85) Without loss of generality, it suffices to prove FLT for 4 and for every odd prime $p \geq 3$. (See "(1.85): Statement and Proof" in Part (2) of this paper, on the web site occampress.com.)

[1] Ribenboim, Paolo, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, N.Y., 1979, p. 226.

Definition of "Minimum Counterexample"

Assuming that there exists x, y, z, n such that $x^n + y^n = z^n$, then, without loss of of generality, we let $n = p$, the smallest such odd prime (see "(1.85): Statement and Proof" in Part (2) of this paper, on the web site occampress.com..) We will often write p instead of n when referring to an assumed counterexample.

If there is more than one triple $<x, y, z>$ such that x, y, z are elements of a counterexample[1] with exponent p, then we choose the $<x, y, z>$ having the minimum z. If there is more than one such triple, then we choose the $<x, y, z>$ having the minimum y. Clearly, there can only be one such triple. We call that triple, and exponent p, the "minimum counterxample". From now on in this paper, unless stated otherwise, the term "counterexample" will always mean "minimum counterexample".

"Lemma 4.0.5" on page 16 shows that, for given x, y, z, there can be at most one prime p such that $x^p + y^p = z^p$.

Lemma 0.0

If $x^p + y^p = z^p$, then $x + y > z$.

Proof see "Lemma 0.0: Statement and Proof" in Part (2) of this paper on the web site occampress.com.

Students of the phenomenon of mathematical intuition might be interested to know that from the moment the author realized this simple fact, he was convinced this would be part of a "simple" proof of FLT if he was able to discover one. The author has no explanation for his conviction, nor does he claim that his conviction will be vindicated.

There are some tempting, very simple possible proofs based on Lemma 0.0. Unfortunately, these are wrong. Here is an example:

If x, y, z are constituents of a counterexample to FLT, then Lemma 0.0 implies that $x + y - z = d$, where d is an integer. However, d must contain a factor p (parts (a) and (b) of "Lemma 0.2: Statement and Proof" in Part (2) of this paper on occampress.com). We then have $x + y \equiv z \bmod p$, hence, by Fermat's Little Theorem, $x^p + y^p \equiv z^p \bmod p$ Thus we do not have a contradiction by which to prove that $x^p + y^p \neq z^p$.

(If p were larger than $x + y$ and of z, then $x + y$ *not* $\equiv z \bmod p$, because there would be no multiple of p such that $x + y + d$ (which contains a factor p) $= z$. In that case, by Fermat's Little Theorem, we would have $x^p + y^p$ *not* $\equiv z^p \bmod p$ hence a contradiction to our assumption that a counterexample exists.

However it was proved in the 19th century[2] that $x > p$.)

Remark

By the contrapositive of Lemma 0.0, if $x + y \leq z$, then x, y, z cannot be elements of a counter-

[1] At least as of the late 1970s, little was known about the set of all $<x, y, z>$ such that x, y, z are elements of a counterexample with minimum exponent p. See, e.g., Ribenboim, Paolo, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, N.Y., p. 232.

[2] Ribenboim, Paolo, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, N.Y., 1979, p. 226

example.

Lemma 0.2

If $x^p + y^p = z^p$, then

(a) $x + y - z = Kdef$, where $K \geq 1$, $d \geq 1$, $e, f > 1$;

(b) $Kdef$ contains the factors 2 and p;

(c) d is a factor of x;
e is a factor of y;
f is a factor of z;
$(d, e, f) = 1$;

(d) if $x^k + y^k - z^k \equiv 0 \bmod k$, where k is a prime, $3 \leq k < p$, then def contains a factor k.

(e) $p < 1/30(x)$. Thus, prior to Wiles' proof of FLT, the smallest x in a counterexample was at least 3,750,000.

(f) $x + y \equiv z \bmod p$.

Proof: see "Lemma 0.2: Statement and Proof" in Part (2) of this paper, on the web site occampress.com.

Lemma 0.3

If k is an odd prime, then $(x + y - z)^k \equiv x^k + y^k - z^k$ *mod k.*

Proof: see "Lemma 0.3: Statement and Proof" in Part (2) of this paper, on the web site occampress.com.

Lemma 0.5.

If $x^2 + y^2 = z^2$, *then x, y, z cannot be elements of a counterexample.*

Proof: see "Lemma 0.5: Statement and Proof" in Part (2) of this paper, on the web site occampress.com.

Lemma 0.6

If FLT is true for the exponent n, then it is true for all multiples of n.

Proof: see "Lemma 0.6: Statement and Proof" in Part (2) of this paper, on the web site occampress.com

Lemma 1.0.

(a) $p < x < y < z$.

(b) $z < x + y < 2y < 2z$.

Proof: see "Lemma 1.0: Statement and Proof" in Part (2) of this paper, on the web site occampress.com.

Lemma 1.5.

Let x, y, z, p be elements of the minimum counterexample. Then for all k, $1 \le k < p$*, k real and not merely integral:*

(a) $x^k + y^k > z^k$, i.e., $x^k + y^k - z^k > 0$; [1]

(b) $x^k + y^k - z^k < x^k$;

(c) $x^k + y^k$ *increases monotonically with increasing* k;

(d) z^k *increases monotonically with increasing* k;

(e) $(x^k + y^k)/z^k > (x^{k+1} + y^{k+1})/z^{k+1}$.

(f) *Let* $f(k) = x^k + y^k - z^k$. Then the slope of f, namely, $x^k(\ln x) + y^k(\ln y) - z^k(\ln z)$, is positive for all k, where $1 \le k < p - 1$, *k real and not merely integral. Thus* $x^k + y^k - z^k < x^{k+1} + y^{k+1} - z^{k+1}$ for integral k, $1 \le k \le p - 2$.

(g) $x^k + y^k - z^k \ge Kdef + k - 1$, where here k is integral and $Kdef$ is as defined in "Lemma 0.2" on page 14. Hence, in particular, since the maximum of the function $x^k + y^k - z^k$ occurs at $p - 1 \le k < p$, it has value $\ge Kdef + p - 2$.

(h) $x^k < y^k < z^k < x^k + y^k < 2y^k < 2z^k$

(i) Let $f(k)$ be as defined in Part (f). Then $f(k + 1) < f(k)$ for all $k > p$.

(j) If $k \ne k'$, then $f(k) \ne f(k')$.

Proof: see "Lemma 1.5: Statement and Proof" in Part (2) of this paper, on the web site occampress.com.

Lemma 1.95.

Let x, y, z, be elements of the minimum counterexample $x^p + y^p = z^p$ *to FLT. Then for all* $k > p$, $x^k + y^k < z^k$.

Proof: see "Lemma 1.95: Statement and Proof" in Part (2) of this paper, on the web site occampress.com.

Lemma 1.97[2]

Let x, y, z, be elements of a counterexample $x^{(p = n+1)} + y^{(p = n+1)} = z^{(p = n+1)}$ *to FLT, where* $p = n + 1$ *is the smallest such exponent. Then*

$$\lim_{k \to \infty} \frac{x^k + y^k}{z^k} = 0$$

[1] Part (a) shows that $x^2 + y^2$ and z^2 cannot form a Pythagorean triple. That is, it cannot be the case that $x^2 + y^2 = z^2$.

[2] A young mathematician has written us that Lemma 1.97 "bears a major resemblance to what is known as the ABC Conjecture, ... a long unsolved problem in additive number theory... The ABC Conjecture almost proves FLT in the sense that if ABC is true, then for all *n sufficiently large*, $x^n + y^n = z^n$ has no integer solutions. See for instance mathworld.wolfram.com/abcconjecture.html."

Proof: see "Lemma 1.97: Statement and Proof" in Part (2) of this paper, on the web site occampress.com .

Lemma 2.0

$z < 2y$.

Proof: see "Lemma 2.0: Statement and Proof" in Part (2) of this paper, on the web site occampress.com.

Lemma 2.5

$z < x^2$.

Proof: Proved by Perisastri in 1969. — Ribenboim, op. cit., p. 226.

Constraints on the Prime *p* in a Counterexample

Lemma 4.0.

Assume a counterexample $x^p + y^p = z^p$ exists. Then p cannot be a member of a certain infinite set of primes.

Proof: see "Lemma 4.0: Statement and Proof" in Part (2) of this paper, on the web site occampress.com.

A young mathematician stated and proved the following, stronger version of Lemma 4.0. (The proof given here is a slightly edited version of the original. Any errors are entirely our responsibility.)

Lemma 4.0.5

Assume a counterexample $x^p + y^p = z^p$ exists. Then p can be at most one prime.

Proof: see "Lemma 4.0.5: Statement and Proof" in Part (2) of this paper, on the web site occampress.com.

Remark on Lemmas 4.0 and 4.0.5. It is important not to misunderstand what these lemmas establish. Suppose that someone announced (before 1990), "I have three numbers, x, y, z, that are elements of a counterexample to FLT!" We know now that the person would have been mistaken, but let us consider several possible responses to the announcement.

(1) A person knowing only that a counterexample would have to involve a prime exponent, but knowing none of the results establishing exponents for which FLT had been proved true, might have responded, "How interesting! The exponent can be any positive prime! Or perhaps there are several prime exponents for each of which x, y, z are the elements of a counterexample."

(2) A person who knew the results concerning exponents might have instead responded, "How

interesting! The exponent can be any prime greater than 125,000. Or perhaps there are several prime exponents in this range, for each of which x, y, z are the elements of a counterexample."

(3) A person who knew what the person in (2) knew, plus Lemma 4.0.5, might have responded, "How interesting! The exponent must be one and only one prime greater then 125,000."

(4) Finally, a person who knew what the person in (3) knew, plus Lemma 4.0, might have responded, "How interesting! The exponent must be one and only one prime greater than 125,000 that is not excluded by Lemma 4.0."

Bertrand's Postulate

This postulate states that if z is a positive integer, then there exists a prime q such that $z < q < 2z$. The proof can be found in most elementary number theory textbooks.

The "Smaller Prime" Lemma

If

$$u = p_1^{e_1} p_2^{e_2} \ldots p_n^{e_n}$$

where $n \geq 2$, *is a product of powers of* successive *primes* p_i, *then there exists a prime* p_j *such that* $p_j < u$ *and* $(p_j, u) = 1$.

Proof:

The product of any two successive primes $p_i^{e_i} p_{i+1}^{e_{i+1}}$ is greater than $2p_i^{e_i}$ and therefore, by "Bertrand's Postulate" on page 17 there is a prime p_j between $p_1^{e_1}$ and $p_2^{e_2}$. And similarly for other successive primes in u. □

Remark 1

Obviously, if u is merely a product of powers of primes, not necessarily successive primes, our Lemma holds, because then a prime that is not included in the product is the prime p_j.

Remark 2

Observe that this Lemma does *not* show that if p, x, y, z are elements of a counterexample to FLT, and hence that $p < x < y < z$ ("Lemma 1.0." on page 14), there exists a prime q such that $(x, q) = (y, q) = (z, q) = 1$ (such a prime is called a *prime appropriate modulus* in Part (4) of this paper, on occampress.com), and such that $q < p$. The reason is that since $p < x$ it is possible that all primes $\leq p$ are factors of x, y, and z.

An Elementary Question and Its Answer

Before we proceed, we should ask a question which it is hard to believe was not asked, and answered, at the very latest in the 19th century, as soon as the notion of a field of numbers had been formalized. (Informally, a field is a set of numbers that behaves "like" the rationals under addition, subtraction, multiplication, and division, except that the field may or may not have the property of unique factorization into primes.) The only reason we ask the question here is that we have not come across it in the FLT literature we have examined thus far. The question is simply this:

Does there exist a field F in which a non-trivial factorization of the form (homogeneous polynomial) $P = x^p + y^p - z^p$ exists, and if so, what are all such fields, and what are the factorizations in each such field?

The importance of the question lies simply in this: (1) if a counterexample exists, then $P = 0$; (2) if a factorization exists, then at least one of the factors of P must = 0. From the latter fact, it might be possible to derive a contradiction. For example, if all factors of P are of the form $(x + r(f(y, z)))$, where r is an irrational number, e.g., a complex root of 1, and $f(y, z)$ is a rational expression in y, z, then we would have a proof of FLT, because this would imply that $x = -r(f(y, z)))$ is an irrational number, contrary to the requirements of FLT.

But as a mathematician has pointed out to us, there does not exist a non-trivial factorization of P over the fields we are interested in (i.e., number fields of characteristic 0). Furthermore, nothing about the existence or non-existence of counterexamples can be inferred from this fact.

Fermat's "Method of Infinite Descent"

"Fermat invented the method of infinite descent and it was an invention of which he was extremely proud. In a long letter written toward the end of his life he summarized his discoveries in number theory and he stated very definitely that all his proofs used this method. Briefly put, the method proves that certain properties or relations are impossible for whole numbers by proving that if they hold for any numbers they would hold for some smaller numbers; then, by the same argument, they would hold for some numbers that were smaller still, and so forth *ad infinitum*, which is impossible because a sequence of positive whole numbers cannot decrease indefinitely."
— Edwards, Harold M., *Fermat's Last Theorem*, Springer-Verlag, N.Y., 1977, p. 8.

The Vertical Approach described above under "Brief Summary of Approaches Described in This Paper" on page 9 can be run in the "downward" direction as well as the upward, and in that case it becomes similar to Fermat's method of infinite descent. This downward-direction approach is discussed briefly under "Approaches via The "Lines-and-Circles" Model of Congruence" on page 21, and then in more detail in "Approaches via The 'Lines-and-Circles' Model of Congruence in Part (4) of this paper, on the web site www.occampress.com. The section "Two Ways to Implement a Method of Infinite Descent" in Part (4) shows how two elementary lemmas can be used to implement this technique. In light of Fermat's statement that all his proofs used the method of infinite descent, which then must be taken to include his claimed proof of FLT, it seems appropriate that we thoroughly explore any approach that is similar to his method.

Case I and Case II of FLT

In the literature, Case I of FLT is defined as that in which the exponent p in an assumed counterexample does not divide x, y, or z. Case II is defined as that in which p divides exactly one of x, y, or z.

At the time of this writing, we have not attempted to deal with these Cases.

First Approach Via the Binomial Theorem

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.

(Another version of this strategy can be found in "Approach Using Inner Products" on page 32.)

Remark

This Approach is similar to several in Part (4) of this paper, on occampress.com, but those approaches are based on the Fixed-Set, that is, expressions $a^k + b^k - c^k$ that have the same value whether counterexamples exist or not. Thus, since prior to Wiles' proof of FLT, it was known that FLT was true for all primes less than 125,000, for any positive integers a, b, c, and any $k <$ 125,000, $a^k + b^k - c^k$ had the same value whether counterexamples existed or not.

Second Approach Via the Binomial Theorem

We know that, if a counterexample $x^p + y^p = z^p$ exists, then $x + y > z$ ("Lemma 0.0" on page 13) and, in fact, that $x + y = z + 30pK$, where $K \geq 1$ (Lemma 0.2 Statement and Proof", Part (2) of this paper, on occampress.com). Therefore it follows that:

(0)
$(x + y)^p = (z + 30pK)^p$**.**

By the binomial theorem, we have

(1)
$x^p + A + y^p = z^p + 30p^2KR,$
where $R >$ 1.

By assumption that $x^p + y^p = z^p$ is a minimum counterexample, this yields

(2)
$A\ =\ xyU =\ 30p^2KR.$

Assume that p does not divide x or y. Then p divides U. Unfortunately, it is possible that U contains one or more additional factors p, and so we cannot claim a contradiction resulting from a different number of factors p in the left- and right-hand sides.

We must now consider the case that p does in fact divide one of x or y. (It cannot therefore divide z). Then by the binomial theorem, we have, from (0),

(3)

$$\binom{p}{1}x^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \binom{p}{3}x^{p-3}y^3 + \ldots + \binom{p}{p-1}x^1y^{p-1} =$$

$$\binom{p}{1}z^{p-1}(30pK) + \binom{p}{2}z^{p-2}(30pK)^2 + \ldots + \binom{p}{p-1}z^1(30pK)^{p-1} + (30pK)^p$$

In order to make the first term on the right-hand side equal the first term on the left-hand side, it must be that

(4)

$$30pK = \frac{x^{p-1}y}{z^{p-1}}$$

However, as the reader can easily verify, this value of $30pK$ will not make the second term on the right-hand side equal the second term on the left-hand side, and similarly for the third, fourth,... etc. terms. Furthermore, it is not necessary that the left-hand side of (2) equal the right-hand side on a term-by-term basis. We observe in passing that (4) implies that $30pK < y$.

In passing, we also observe that x is a factor of A in (1). On the right-hand side, we know that $x \neq p$ (because $p < x$ by "Lemma 1.0." on page 14) and that x cannot divide z (because by assumption (x, y) = (y, z) = (x, z) = 1 ((1.5 under "Initial Assumptions, Definitions, and Properties of Numbers Involved" on page 12). Furthermore, x cannot equal $30pK$ because since $x + y = z + 30pK$ (Lemma 0.2 Statement and Proof", Part (2) of this paper, on occampress.com) that would imply $x + y = z + x$, or $y = z$, which is impossible. So x must be a factor of the right-hand side of (1) for another reason, namely, that the terms on the right-hand side just happen to add up to an integer that has x as a factor.

Similarly for y.

Vertical Approaches Based on Congruences

Approaches via The "Lines-and-Circles" Model of Congruence

We begin with an overview of all these approaches. Our goal is to convey, as clearly as possible, underlying ideas. Details are given in Part (4) of this paper, on the web site www.occampress.com.

Definition of "Line-and-Circles" Model of Congruence

All approaches based on congruences are motivated by a "geometrical" model of congruence. In this model, an infinite sequence of circles are positioned at equal distances, one above the other (see Fig. 1).

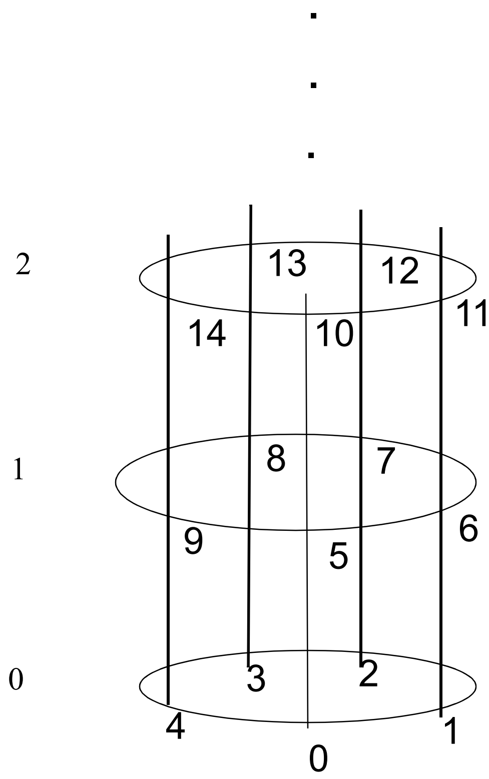

Fig. 1. "Geometrical" model of positive integers congruent mod 5.

For the modulus *m*, each circle is divided equally into *m* segments as shown (here, *m* = 5). Vertical lines pass through the start of each segment. All integers congruent to a given minimum residue *r* mod *m* lie on the same vertical line, with *r* at the start of the line.

We refer to the circles as *levels mod m* (or merely *levels* when *m* is understood), and number them 0, 1, 2, ... beginning with the lowest one. The level numbers are the quotients of all numbers on that level when divided by *m*. Thus, in our example, 14 ÷ 5 yields the quotient 2 and the remainder 4, so 14 is on level 2 and line 4. We sometimes refer to level 0 as the *base level mod m* (or merely the *base level* when *m* is understood).

Two facts lie at the basis of all our Approaches via the "lines-and-circles" model of congruence:

(1) that, for each modulus *m*, each positive integer *u* has a "location" relative to that modulus. This location is given by the ordered pair <*level*, *line*> which can be regarded as the "address" of *u* mod *m*. Thus, in our previous example, the address of 14 mod 5 is given by <2, 4>. We will be concerned with ordered triples $<a^k, b^k, c^k>$, where *a*, *b*, *c*, *k* are positive integers. In particular, we will be concerned with $<x^p, y^p, z^p>$, where $x^p + y^p = z^p$ is an assumed minimum counterexample, and with all $<x^k, y^k, z^k>$, where $k \geq 1$ and $k \neq p$. At times, for reasons that will become clear, we will also be concerned with ordered pairs, $<x^k + y^k, z^k>$.

(2) that, for a given *u*, as the modulus *m* increases, the location of *u* descends in the lines-and-circles model for each modulus. There exists a minimum *m* such that $u < m$. We say that u

touches down at m. Clearly, $u < m'$ for all $m' > m$. Informally, we say "once down, always down."

Summary of Approaches via the "Lines-and-Circles" Model of Congruence

We here try merely to suggest the underlying idea for each Approach. Details can be found in the indicated sections of Part (4) of this paper, on the web site www.occampress.com.

Approaches Type I through VI

(Type I) Show that if $x^p + y^p = z^p$, then a contradiction arises involving $a^p + b^p$, c^p, where $a \leq x$, $b \leq y$, $c \leq z$, and $a \equiv x$, $b \equiv y$, $c \equiv z \bmod m$.

For details, see sections containing "Type I" in Part (4) of this paper.

(Type II) Show that if $x^p + y^p = z^p$ then a contradiction arises involving $x^r + y^r$, z^r , where $2 < r < p$.

For details, see sections containing "Type II" in Part (4) of this paper.

(Type III) Show that if $x^p + y^p = z^p$, then $<x^p + y^p, z^p>$ is an element of a non-congruent **C**-set. (This is impossible because (informally) non-congruence implies inequality.)

For details, see sections containing "Type III" in Part (4) of this paper.

(Type IV) Show that by considering all multiples of all powers of positive integers u, v, w, we are led to a contradiction.

For details, see sections containing "Type IV" in Part (4) of this paper.

(Type V) Show that a contradiction arises from the set of congruences and non-congruences resulting from all **C**-set elements $<x^p + y^p, z^p>$.

For details, see sections containing "Type V" in Part (4) of this paper.

(Type VI) Show that the assumption of a counterexample implies a contradiction in the U_k, where $x^k + y^k - z^k = U_k$,, and $k \neq p$.

For details, see sections in Part (4) of this paper.

The "Pushing-Up" Approach

Assume a counterexample, $x^p + y^p = z^p$, exists. Then show that the counterexample never "touches down", that is, show that there is no modulus m such that $x^p + y^p$, and z^p are each less than m. This would imply that the counterexample does not exist.

For details, see "Original Motivation for Approaches via The "Lines-and-Circles" Model of Congruence" in Part (4) of this paper.

Another Approach

The following was motivated by an unpublished paper by, and subsequent discussions with, Richard Van Elburg, These discussions ended in January, 2013.

If there is one Approach that has been favored by amateurs over the years beyond those that attempt to use the Pythagorean Theorem it is probably the following: express two of x, y, z in terms of the third, then substitute into the FLT equation

$$x^p + y^p = z^p \tag{1}$$

and try to derive a contradiction. Thus, for example, we might let $x = z - h$, and $y = z - k$. This Approach invites the use of at least two elementary facts that most amateurs are probably familiar with, namely, Fermat's Little Theorem and the binomial theorem. It is reasonable to assume that Fermat knew of both when he attempted to prove FLT.

As far as we know, a report on an exhaustive investigation of such an Approach has never been published.

We begin by pointing out that there is always the null substitution, in which we work directly from (1). For each pair of definitions — for example, $x = z - h$, and $y = z - k$.— there are three more possible substitutions into (1): the substitution of only one definition into (1) (two possibilities), and the substitution of both definitions simultaneously into (1) (one possibility).

In this Appendix, we will investigate only the null substitution.

Since by the assumed properties of a counterexample, $(x, y) = (y, z) = (x, z) = 1$, we know that p divides at most one of x, y, z. If p does not divide x, y, or z, we have, by Fermat's Little Theorem,

$$x^p \equiv x \bmod p,\ y^p \equiv y \bmod p, \text{ and } z^p \equiv z \bmod p, \tag{2}$$

which, by definition of congruence, implies

$x^p = x + ip$, $y^p = y + jp$, and $z^p = z + kp$, where i, j, k are positive integers.

Equation (1) then implies

$x + ip + y + jp = z + kp$, or

$$\mathrm{x} + y + (i + j - k)p = z. \tag{3}$$

Since i, j, k are each positive, and since, by "Lemma 0.0" on page 13, $x + y > z$, equation (3) can only hold if $i + j < k$. We have already established (3) in part (a) of "Lemma 0.2" on page 14.

In terms of the lines-and-circles model of congruence (see "Approaches via The 'Lines-and-Circles' Model of Congruence" in Part (4) of this paper, on the web site www.occampress.com) we have established the following:

Regardless whether p divides none or one of x, y, z:

x and x^p lie on the same line mod p,
y and y^p lie on the same line mod p,
z and z^p lie on the same line mod p, and
$x + y$ and z lie on the same line mod p.

Since $p < x < y < z$ (by part (a) of "Lemma 1.0." on page 14), we therefore can state, if "(1.91) (c)" in Part (2) of this paper, on the web site occampress.com, holds for the Trivial Extension of

Fermat's Little Theorem, that there exist u, v, w such that:

$u < x$, $v < y$, $w < z$,
u, v, w, $< p$ (we don't know if $u + v < p$),
$x \equiv u \; mod \; p,$
$y \equiv v \; mod \; p,$
$z \equiv w \; mod \; p,$
$u^p + v^p \equiv w^p \; mod \; p \; and$
$z^p \equiv u^p \; mod \; p,$
$y^r \equiv v^p$ mod p, and
$z^p \equiv w^p \; mod \; p.$

The above statements concerning u, v, w are ground we have trodden, so far without result, in the sections on Vertical Approaches using the lines-and-circles model of congruence. However, in those sections we did not use p as the modulus. If we could prove that $u + v$ is not $\equiv w$ mod p, we would have our proof of FLT, because that would imply that $x + y$ is not $\equiv z$ mod p, a contradiction. In the following paragraphs, we investigate ways of proving that $u + v$ is not $\equiv w$ mod p.

Statement (2) implies

$$x + y \equiv z \; mod \; p. \tag{4}$$

By part (a) of "Lemma 1.5." on page 15we know that $x + y > z$, so, by definition of congruence, statement (4) implies that there exists a positive m such that

$$x + y - mp = z. \tag{5}$$

Since, by part (a) of "Lemma 1.0." on page 14, $p < x < y < z$, and by definition of congruence, we know there exist positive integers i, j, k such that

$u + ip = x,$
$v + jp = y,$
$w + kp = z,$

where u, v, w are each less than p. (6)

Combining the statements in (6) with statement (5) we get:

$$u + ip + v + jp - mp = w + kp. \tag{7}$$

There are now two possibilities:

(A) $u + v > p$, or
(B) $u + v \leq p.$

In the case of (A), there are now two further possibilities:

(A.1) $u + v = w$, or
(A.2) $u + v \neq w$.

(A.1) is ruled out by the fact that $c < p$ ((6)).

So (A.2) holds, and this is one of the possibilities we are hoping for.

Now let us consider (B). There are now two further possibilities:

(B.1) $u + v < w$, or
(B.2) $u + v = w$.

If (B.1) holds, then, again, we have one of the possibilities we are hoping for.

So we come to the only remaining possibility, namely, (B.2). We see in (7) that if $u + v = w$ then $i + j - m$ must equal k. If we can show that is impossible, then we have a proof of FLT.

Vertical Approaches by Induction on Inequalities

"Arithmetical" Version of the Approach by Induction on Inequalities

Brief, Simple Description of the "Arithmetical" Version

The reader will recall our "Vertical Approach" to a proof of FLT as described under "Brief Summary of Approaches Described in This Paper" on page 9:

"[In this Approach], 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, 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 $x^n + y^n$ with z^n for $n = 3$, then for $n = 4$, then for $n = 5$, etc."

In this sub-section, we discover some facts about the sequence of FLT inequalities,

$x^3 + y^3 \neq z^3$,
$x^4 + y^4 \neq z^4$,

...

$x^n + y^n \neq z^n$, and then, following the assumed equality,
$x^{(p = n+1)} + y^{(p = n+1)} = z^{(p = n+1)}$, the further inequalities,
$x^{n+2} + y^{n+2} \neq z^{n+2}$,
$x^{n+3} + y^{n+3} \neq z^{n+3}$,
...

We first state the following basic facts about the FLT inequalities. The formal statement of each lemma, and the proof, is given in "Appendix F — Statement and Proof of Certain Numbered Statements and of Lemmas" on page 73.

for all k, $1 \leq k < n + 1$:
$x^k + y^k > z^k$ (part (a) of "Lemma 1.5." on page 15);
$(x^k + y^k)/z^k > (x^{k+1} + y^{k+1})/z^{k+1}$ (part (e) of "Lemma 1.5." on page 15).

for all $k > p = n + 1$:
$x^k + y^k < z^k$ ("Lemma 1.95." on page 15);
$lim\ k \rightarrow \infty$, $(x^k + y^k)/z^k = 0$ ("Lemma 1.97" on page 15).

One answer to the question of the maximum size of $p = n+1$ in a counterexample to FLT is given by Lemma 1.0, namely, p must be $< x$.

We now discuss a possible approach for proving FLT that uses ratios between the FLT inequalities.

Approach Using Ratios Between FLT Inequalities
First Implementation of Approach

We begin by reminding the reader of the sequence of inequalities, followed by an inequality, that lies at the basis of our Vertical approach to a proof of FLT. The sequence of inequalities is:

$x + y \neq z$,
$x^2 + y^2 \neq z^2$,
$x^3 + y^3 \neq z^3$,
$x^4 + y^4 \neq z^4$,
...
$x^n + y^n \neq z^n$, where $n = p - 1$.

The assumed equality is:
$x^{(p = n+1)} + y^{(p = n+1)} = z^{(p = n+1)}$.

Part (a) of "Lemma 1.5." on page 15 states that for all k, $1 \leq k < p = n + 1$: $x^k + y^k > z^k$
We therefore write

$$\frac{x^k + y^k}{z^k} > 1$$

or

$$\frac{x^k}{z^k} + \frac{y^k}{z^k} > 1$$

"Lemma 1.0." on page 14 states that $p < x < y < z$, so for all k, $1 \leq k < p = n + 1$, we know that

$$\frac{u^k}{z^k} < 1$$

where $u = x$ or y. Furthermore, as k increases each of the fractions x^k/z^k, y^k/z^k grows smaller. In the counterexample case, namely,

$$\frac{x^p}{z^p} + \frac{y^p}{z^p} = 1$$

either both x^p/z^p, $y^p/z^p = 1/2$, or one of x^p/z^p, y^p/z^p must be $< 1/2$.

We now investigate the application of some known constraints on x, y, and z to the above fractions. To begin with, we know[1] that

$$y < z < y\left(1 + \frac{1}{p}\right)$$

So a lower bound[2] (unfortunately, not an upper bound) on y/z is

$$\frac{y}{y\left(1 + \frac{1}{p}\right)} = \frac{1}{\left(1 + \frac{1}{p}\right)} = \frac{p}{(p+1)}$$

What can we say about

$$\left(\frac{p}{(p+1)}\right)^p$$

for large p? Using a pocket calculator we find, for example, that

$$\left(\frac{37}{(37+1)}\right)^{37} \approx 0.373$$

and that, for example

[1] Ribenboim, Paolo, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, N.Y., 1979, p. 226

[2] A reader has written us: "The lower bound you develop on y/z could be replaced with a stronger lower bound. Assume $x < y < z$. Then since $(x/z)^p + (y/z)^p = 1$, $(y/z)^p \geq 1/2$, or $y/z \geq (1/2)^{(1/p)}$. This bound is between 1/2 (for $p = 1$) and 1 (as $p \rightarrow \infty$), and is monotonically increasing with p. On the other hand, the bound you use, $y/z > (p/(p+1))^p$ is between 1/2 (for $p = 1$) and $1/e$ (as $p \rightarrow \infty$), and is probably... monotocally decreasing with p."

$$\left(\frac{503}{(503+1)}\right)^{503} \approx 0.368$$

Since $x/z < y/z$, it seems that no counterexample is possible for y/z near the above lower bound, because in these cases

$$\frac{x^p}{z^p} + \frac{y^p}{z^p} < 1$$

The upper bound on $y/z = y/(y + 1)$. But since, by "Lemma 1.0." on page 14, $p < x < y$, it is possible that

$$\left(\frac{y}{(y+1)}\right)^{p} > 1/2$$

For example,

$$\left(\frac{503}{(503+1)}\right)^{257} \approx 0.600$$

But even if x were as large as, say, 405, $(405/504)^{257}$ is so small that a counterexample with $x = 405$, $y = 503$, $z = 504$, $p = 257$ is impossible, as the reader can verify.

Other constraints on x, y, z can be found in Lecture XI, "Estimates", pp. 225-243 in the above-cited work by Ribenboim. For example, we find that $z < x^2$ and $z - x > 2^p p^{2p}$. Let us apply the first of these relations to our example of $y = 503$, $z = 504$. Since $22^2 = 484$ and $23^2 = 529$, we see that x must be ≥ 23. Let $p = 19$. Then

$$\left(\frac{503}{(503+1)}\right)^{19} \approx 0.963$$

But even if x were as large as, say, 105 (which, of course, it couldn't be, given that $z - x > 2^p p^{2p}$), we find that

$$\left(\frac{105}{(503+1)}\right)^{19}$$

is so small as to make a counterexample impossible with $x = 105$, $y = 503$, $z = 504$, $p = 19$.

At the very least, we should use the computer and the above constraints, plus others, to develop a table of non-counterexample 4-tuples $<x, y, z, p>$ including, of course, $p > 125{,}00$, the lower bound on p in a counterexample as of the early nineties.

Second Implementation of Approach

Part (f) of "Lemma 1.5." on page 15 states that the function $x^k + y^k - z^k$ is increasing for $1 \leq k$

$\leq p-1$, k real and not merely integral. But in order for a counterexample to exist, namely, for $x^k + y^k - z^k = 0$, there must exist a c, $p-1 < c < p$ such that for k, $c < k \leq p$, the function must be decreasing, or, in other words, the derivative $x^k(\ln x) + y^k(\ln y) - z^k(\ln z)$ of the function must be less than 0 . The following facts might enable us to accomplish a proof by contradiction. Some thoughts on possibilities are given after the following list of facts.

(1)
$x^c(\ln x) + y^c(\ln y) - z^c(\ln z) = 0$, i.e.,

$$\frac{x^c(\ln x)}{z^c(\ln z)} + \frac{y^c(\ln y)}{z^c(\ln z)} = 1$$

($k = c$ is the point at which the tangent to the function $x^k + y^k - z^k = 0$ is horizontal, i.e., the point at which the function is no longer increasing.)

(2)
Since the function $x^k + y^k - z^k$ is monotonically increasing from $k = 1$ to $k = p - 1$ (part (f) of "Lemma 1.5." on page 15), the value of the function at $k = p - 1$ must be $\geq Kdef + p - 1$("Lemma 0.2" on page 14).

(3)
$x^k(\ln x) + y^k(\ln y) - z^k(\ln z) < 0$, $c < k \leq p$, i.e.,

$$\left(\frac{x^k(\ln x)}{z^k(\ln z)} + \frac{y^k(\ln y)}{z^k(\ln z)}\right) < 1$$

(4)
$x^k + y^k - z^k > 0$, $c < k < p$, i.e.,

$$\left(\frac{x^k}{z^k} + \frac{y^k}{z^k}\right) > 1$$

(5)
$\ln u/\ln v > u/v$, u, v, $> e$. (See proof of "Lemma 1.5." on page 15.)

(6)
$x^p + y^p - z^p = 0$.

A reader has pointed out that for x, y, z such that $x < y < z$ and $x + y > z$, a continuous function $x^k + y^k - z^k$ of k can be defined, and that this function will have the property that the function increases to a certain maximum value, then decreases thereafter, crossing the k axis at some point, i.e., at some point has the value 0.

To which we reply that, although this is true, in the case when x, y, z are elements of a counterexample, descent from the maximum value to 0 occurs over a range of k that is less than 2 units. It took about $p - 1$ units for the function to reach its maximum, and then less than 2 units for it to return to 0. Yet neither the function nor its derivative $x^k (\ln x) + y^k (\ln y) - z^k (\ln z)$ suggest that such a rapid change in the derivative occurs at some point.

Is this the basis for a proof of FLT by contradiction?

Approach Using Basic Algebra

1. Assume a counterexample $x^p + y^p - z^p = 0$ to FLT exists. Prior to Wiles' proof of FLT, it was known that FLT is true for all k where $3 \leq k < 4{,}000{,}000$, so assume p is a prime > 4,000,000.

2. Now consider

(1)
$$x^{(p-1)}(x-1) + y^{(p-1)}(y-1) - z^{(p-1)}(z-1)$$

It is equal to $x^p - x^{(p-1)} + y^p - y^{(p-1)} - z^p - z^{(p-1)}$, which, given our counterexample, is equal to

(2)
$$-x^{(p-1)} - y^{(p-1)} + z^{(p-1)}.$$

3. But comparing (2) with (1), which are equal, we must conclude that

(3)
$$(x-1) = -1; \quad (y-1) = -1. \text{ and } (z-1) = -1.$$

(We are aware that, in general, when dealing with integers, it is *not* the case that

$Ag + Bh = g + h$ implies only that $A = 1$ and $B = 1$. Consider, e.g., that

$(5)(3) + (-2)(4) = 7 = 3 + 4$, and neither 5 nor -2 equal 1.

But our case is different, because our entities in (1) and (2) are not integers, and because in (1) and (2) there are no equivalents for A and B.)

4.

And therefore (3) implies that $x = 0$, $y = 0$, and $z = 0$, which, of course, is false.

So our assumption has led to a contradiction, and therefore FLT is true.

Approach Using Inner Products

Assume a counterexample $x^p + y^p = z^p$ exists, where p is prime, and $(x, y) = (x, z) = (y, z) = 1$, and p 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 $<(x^{p-1}, y^{p-1}, z^{p-1}), (x, y, -z)> = 0$. (We can also express it as $<(x^{p-k}, y^{p-k}, z^{p-k}), (x^k, y^k, -z^k)> = 0$, where $1 \le k \le p-1$.)

(The inner product is a function on vector spaces. We do not know if the two terms in each of our inner products are elements of a vector space. But that does not matter, since we are only using the inner products as forms of calculations. We are not, for example, claiming that because our inner products = 0, the angle between the pair of terms is 90°, which would be the case if the terms were elements of a vector space.)

Now FLT is true for all k, where $3 \le k < p$. And this is true whether or not a counterexample exists. In other words, for each of these k, $(x^{p-k})(x^k)$ has one and only one value, whether or not a counterexample exists. And similarly for $(y^{p-k})(y^k)$ and $(z^{p-k})(z^k)$.

But that means $<(x^{p-k}, y^{p-k}, z^{p-k}), (x^k, y^k, -z^k)>$ has the same value, whether or not a counterexample exists. This is not possible. We conclude that a counterexample does not exist. If our reasoning is correct, we have a proof of FLT.

Approaches related to this Approach are the following:
"Approach Using "Neighbor" of Assumed Counterexample" on page 32;
"Approach Using Pythagorean Theorem" on page 33;
"Third Promising Approach to a Simple Proof of FLT", in Appendix A of Part (4) of this paper, on occampress.com;
"Four-Dimensional Cartesian Grid Approach" on page 35 of this file;

Approach Using "Neighbor" of Assumed Counterexample

1. Assume a counterexample $x^p + y^p = z^p$ to Fermat's Last Theorem (FLT) exists, where $(x, y) = (x, z) = (y, z) = 1$ and p is the smallest such p.

2. Because FLT is true for all k, $3 \le k \le (p-1)$, $(x^k + y^k - z^k)$ has one and only one value for each of these k, regardless if a counterexample exists or not.

3. Now the sum $(x^{p-1} + y^{p-1} - z^{p-1}) + x^{p-1}(x-1) + y^{p-1}(y-1) - z^{p-1}(z-1)$ has one and only one value, regardless if a counterexample exists or not.

4. But that sum = $(x^p + y^p - z^p)$, which means that $x^p + y^p - z^p$ has one and only one value, regardless if a counterexample exists or not. But that is absurd, and therefore, a counterexample does not exist.

Approach Using Pythagorean Theorem

1. Any two straight lines of non-zero finite length can be the legs of a right triangle.

2. The Pythagorean theorem applies to all right triangles.

3. Let a, b be any positive integers, and k a positive integer, where $3 \le k$.

Then $a^{k/2}$ and $b^{k/2}$ can be the legs of a right triangle. Therefore, by the Pythagorean theorem,

(1)

$$(a^{k/2})^2 + (b^{k/2})^2 = c^2$$

and thus

(2)

$$a^k + b^k = c^2$$

4. Assume a counterexample $x^p + y^p = z^p$ to Fermat's Last Theorem exists, where $(x, y) = (x, z) = (y, z) = 1$ and p is the smallest such prime p. (Prior to the proof of FLT in the early 1990s, p was known to be greater than 4,000,000.)

5. Then we can write

$(x^{(p/2)})^2 + (y^{(p/2)})^2 = c^2$, i.e.,

(3)

$x^p + y^p = c^2$.

6. So z^p must equal c^2. We know that c^2 is an integer because it is the sum of the positive integers x^p and y^p. It can't be a prime because z^p is not a prime. So it must be a composite.

There are now two possibilities:

(1) $c^2 = (z^{(p/2)})^2 = (z^{(p/2)})\ (z^{(p/2)})$. But this is false because $(z^{(p/2)})^2$ is not a product of primes, as required by a composite integer.

(2) $c^2 = (n)(n)$, where n is a positive integer. But this too is false because z^p is not a square of an integer.

So z^p does not equal c^2, and our assumed counterexample to FLT is false. Hence FLT is true.

.

Is One of the Above Short Approaches, Fermat's "Lost Proof"?

Around 1637, Fermat made a note in the margin of his copy of an ancient number theory text by Diophantus that he was reading, in which he first stated what became known as Fermat's Last Theorem (FLT) (though it was only a conjecture until it was proved by Andrew Wiles in the early 1990s), and then concluded, "I have found a remarkable proof of this fact, but there is not enough space in the margin [of the book] to write it."

For more than 350 years, mathematicians tried unsuccessfully to figure out what Fermat's proof was as they tried to find *any* proof of FLT.

Is the above Approach Fermat's proof? One reason that the answer might be Yes is that Fermat was proud of his discovery of the proof method he called "the method of infinite descent". Here, a counterexample is assumed, and then one shows that there is a smaller positive integer that is a counterexample. And then that there is a smaller positive integer, etc. But this sequence cannot continue forever if the counterexamples are to be positive integers. The contradiction yields a proof.

Now if Fermat assumed a counterexample to FLT existed (see step 1 above) and that p was the smallest exponent in any counterexample, then his method of infinite descent might have prompted him to think of the sequence, $(x^{p-1} + y^{p-1} - z^{p-1})$, $(x^{p-2} + y^{p-2} - z^{p-2})$, ... , $(x^3 + y^3 - z^3)$. He would have recognized that FLT is true for each of these exponents, and that therefore (this would have been the first crucial insight) each expression in the sequence has one and only one value, regardless if a counterexample exists or not.

If he had the second crucial insight, namely, of recognizing that the value of each element of the sequence (apart from the first) is the value of the previous element plus the difference in values between the two elements, he may then have arrived at one of the above Approaches.

Approach Involving Comparing Counterexamples and Non-Counterexamples

This Approach relies on the fact that each term $u^k + v^k - w^k$, where u, v, w, k are positive integers, and k is a exponent for which FLT has been proved true, has the property of remaining the same regardless if a counterexample exists or not. For example, we cannot seriously imagine a professional mathematician saying, prior to Wiles' proof of FLT, things like, "Well, of course we know that $17^3 + 6^3 - 19^3 = -1730$, but if a counterexample is proved to exist, then this might change — the value on the right-hand side might change."

We call the set of terms that remain the same regardless if a counterexample exists or not, the "Fixed-Set" of the problem. Then our Approach has two implementations.

(1) assume a counterexample exists, then show that this implies that an element of the Fixed-Set is changed. Or

(2) assume a counterexample exists, then show that a term that must be changed as a result of the existence of a counterexample, is unchanged. (The latter implementation is used in our proof of the $3x + 1$ Conjecture in the paper "A Solution to the $3x + 1$ Conjecture" on occampress.com.)

We emphasize that *comparing* the two cases in no way implies that the two cases exist simultaneously, which would be absurd.

An example of implementation (1) is "Third Promising Approach to a Simple Proof of FLT", in Appendix A of Part (4) of this paper, on occampress.com (2¼ pages).

Four-Dimensional Cartesian Grid Approach

1. Consider a four-dimensional Cartesian grid such that the point having coordinates (k, a, b, c) is associated with the value of $a^k + b^k - c^k$, where a, b, c, k are positive integers, and $k > 2$. The grid makes it possible to speak of the values associated with *immediately adjacent* points.

2. Prior to Wiles' proof of FLT it was well-known that, if FLT is known to be true for an exponent n (> 2), then there is one and only one value for each $x^n + y^n - z^n$, regardless if a counter-example to FLT exists. (It was also known that if FLT is true for the prime exponent p, it is true for all exponents that are multiples of p (easy proof).)

3. Assume a counterexample $x^p + y^p - z^p = 0$ exists, and assume that p is the smallest such exponent.

Then there is one and only one value for $x^{p-1} + y^{p-1} - z^{p-1}$ regardless if a counterexample to FLT exists.

But then there is one and only one value for $x^{p-1} + y^{p-1} - z^{p-1}$with x^{p-1} replaced by $(x^{p-1})(x)$, (y^{p-1} replaced by y^{p-1}) (y), and z^{p-1} replaced by $(z^{p-1})(z)$.

But that means there is one and only one value for $x^p + y^p - z^p$ regardless if a counterexample exists, which is absurd. This absurdity give s us a proof of FLT.

Approach of Multiplying Fractional Polynomials

If a counterexample exists, then the following are true:

(1)

$$\frac{x^p}{z^p} + \frac{y^p}{z^p} = 1$$

and

(2)

$$x^p + y^p - z^p = 0$$

It is natural to attempt to derive a contradiction using one (or both) of these two facts.

A potentially promising argument is the following.

1. Since for all rationals m it is the case that $(m)(1) = m$, it must be the case that

(3)

$$\left(\frac{x^{p-1}}{z^{p-1}}+\frac{y^{p-1}}{z^{p-1}}\right)\left(\frac{x^{p}}{z^{p}}+\frac{y^{p}}{z^{p}}\right) = \left(\frac{x^{p-1}}{z^{p-1}}+\frac{y^{p-1}}{z^{p-1}}\right)$$

Multiplying out the terms on the left-hand side, we get

(4)

$$\left(\frac{x^{p-1}}{z^{p-1}}+\frac{y^{p-1}}{z^{p-1}}\right)\left(\frac{x^{p}}{z^{p}}+\frac{y^{p}}{z^{p}}\right) = \left(\frac{x^{2p-1}+x^{p-1}y^{p}+y^{p-1}x^{p}+y^{2p-1}}{z^{2p-1}}\right)$$

If the right-hand side of (3) does not equal the right-hand side of (4), we have a proof of FLT. Setting these right-hand sides equal, we have:

(4.5)

$$\frac{x^{p-1}+y^{p-1}}{z^{p-1}} = \frac{x^{2p-1}+x^{p-1}y^{p}+y^{p-1}x^{p}+y^{2p-1}}{z^{2p-1}}$$

or

(5)

$$x^{p-1}+y^{p-1} = \frac{x^{2p-1}+x^{p-1}y^{p}+y^{p-1}x^{p}+y^{2p-1}}{z^{p}}$$

The numerator on the right-hand side is

$$(x^{p}+y^{p})(x^{p-1}+y^{p-1})$$

which makes the right-hand side = the left-hand side, hence no contradiction.

It might be possible to make some progress with this approach by invoking a few of our results, such as $x + y > z$ (Lemma 0.0); $(x^{p-1} + y^{p-1})/z^{p-1} > 1$ (Lemma 1.5); $p < x < y < z < 2y$ (Lemma 2.0); and the fact (easily proven) that if $k > p$, then $(x^{k} + y^{k})/z^{k} < 1$.

Approaches of Multiplying Integer Polynomials

First Approach of Multiplying Integer Polynomials

Before spending time on this sub-section (that is, in "First Approach..."), the reader is urged to read "The Danger of "Null" Approaches" on page 8.

In the course of this research we have spent a fair amount of time trying to derive a contradiction from the multiplication of the following pairs of polynomials:

$(x + y - z)$ and $(x^k + y^k + z^k)$;
$(x + y + z)$ and $(x^k + y^k - z^k)$;
$(x + y + z)$ and $(x^{p-1} + y^{p-1} - z^{p-1})$;
$(x + y - z)$ and $(x^{p-1} + y^{p-1} + z^{p-1})$; and
$(x + y + z)$ and $(x^p + y^p - z^p)$,

For example, consider the product $(x + y - z)(x^{p-1} + y^{p-1} + z^{p-1})$. Since $(x + y - z)$ is positive ("Lemma 0.0" on page 13) and integral, the product must be a positive integer $>$ $(x^{p-1} + y^{p-1} + z^{p-1})$.

.Multiplying out the product, we get:

$(x + y - z)(x^{p-1} + y^{p-1} + z^{p-1}) =$

$$\begin{array}{cccccc} x^p & + & xy^{p-1} & + & xz^{p-1} & + \\ yx^{p-1} & + & y^p & + & yz^{p-1} & + \\ -zx^{p-1} & - & zy^{p-1} & - & z^p. & \end{array}$$

Since, by hypothesis, $x^p + y^p - z^p = 0$, when we collect terms we get:

$x(y^{p-1} + z^{p-1}) + y(x^{p-1} + z^{p-1}) - z(x^{p-1} + y^{p-1})$, or

$$(y - z)x^{p-1} + (x - z)\,y^{p-1} + (x + y)z^{p-1}. \qquad (1)$$

Our original product can be written

$$(x + y - z)x^{p-1} + (x + y - z)y^{p-1} + (x + y - z)z^{p-1} \qquad (2)$$

If (1) ≠ (2), then we have a proof of FLT. Unfortunately, it easy to show that (1) = (2), given our assumption of a counterexample.

Second Approach of Multiplying Integer Polynomials

1. Consider the product $h = (x^k + y^k - z^k)(x^j + y^j - z^j)$, where $k, j \geq 1$, and $k + j = p$, the prime exponent in our assumed counterexample.

We know that $0 < (x^k + y^k - z^k) < x^k$ and $0 < (x^j + y^j - z^j) < x^j$ by part (b) of "Lemma 1.5." on page 15. Thus $0 < h < x^p$. By part (g) of "Lemma 1.5." on page 15, we also know that $h \geq (Kdef + k - 1)((Kdef + j - 1)$.

.

If we can prove that $h \leq\ 0$ or $h \geq x^p$, then this contradiction will give us a proof of FLT. Observe that the first of these conditions on h is merely sufficient for a contradiction, since we have a contradiction if we can prove that h has a value that is less than $(Kdef + k - 1)((Kdef + j - 1)$.

2. Multiplying out the product, we get, for h:

(1)
$h =$
$x^kx^j + x^ky^j - x^kz^j +$
$y^kx^j + y^ky^j - y^kz^j +$
$-z^kx^j - z^ky^j + z^kz^j$.

3. By the conditions on k, j, we have $x^kx^j = x^p$, $y^ky^j = y^p$, and $z^kz^j = z^p$. By assumption of a counterexample, we see that the sum of the three diagonal elements in (1) is $2z^p$.

4. Gathering the positive terms in (1), we have:

(2)
$2z^p + x^ky^j + y^kx^j$.

Gathering the negative terms in (1), we have:

(3)
$-\ (x^kz^j\ + y^kz^j + z^kx^j + z^ky^j) = -\ ((x^k + y^k)\ z^j + (x^j + y^j)\ z^k)$.

5. Let $k = p - 1, j = 1$. Then (2), the expression for the positive terms, becomes

(3)
$2z^p + x^{p-1}y^1\ + y^{p-1}x^1 = 2z^p + xy(x^{p-2} + y^{p-2})$.

By part (a) of "Lemma 1.5." on page 15, we know that $x^{p-2} + y^{p-2} = z^{p-2}\ + Kdef + \geq (p - 3)$. Since it is easily shown[1] that $xy = z + z(y - 1)\ -\ y^2 + Kdefy$ we can write, from (3)

(4)
$2z^p + x^{p-1}y^1\ + y^{p-1}x^1 = 2z^p +\ (z + z(y - 1)\ -\ y^2 + Kdefy)(z^{p-2}\ + Kdef + \geq (p - 3))$:

[1] Simply set $x + y = z + Kdef$ (by part (a) *of* "Lemma 1.5." on page 15), yielding $x = z - y + Kdef$. Then multiply through by y, and set $zy = z + z(y - 1)$.

where "$(\geq u)$" denotes a quantity greater than or equal to the positive integer u.

6. We now expand the expression for the negative terms, (3), with $k = p - 1$, $j = 1$ as for the positive terms. We get

(6)
$$-(x^k z^j + y^k z^j + z^k x^j + z^k y^j) = -((x^{p-1} + y^{p-1})\, z^1 + (x^1 + y^1)\, z^{p-1}).$$

By part (a) of "Lemma 1.5." on page 15, we know that $x^{p-1} + y^{p-1} = z^{p-1} + Kdef + \geq (p - 2)$. So

(7)
$$((x^{p-1} + y^{p-1})\, z^1 = z^p + z(Kdef + >(p - 2)).$$

Similarly, we know that $x^1 + y^1 = z^1 + Kdef$. So

(8)
$$(x^1 + y^1)\, z^{p-1} = z^p + z^{p-1}(Kdef).$$

7. We see immediately that $2z^p$ in the positive terms (4) and $2z^p$ in the negative terms ((7) and (8)) cancel. That leaves 12 terms on the right-hand side of (4). But there are too many uncertainties in the values of some of these terms for us to draw any conclusions about the size of the positive vs. the negative terms in (1).

Third Approach of Multiplying Integer Polynomials

1. It is easy to show that, if a counterexample $x^p + y^p = z^p$ exists, then

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

2. It follows from a basic property of the ring of polynomials that the right-hand side of (1) must be divisible by $(x + y + z)$. If we can show that this is not the case, then that gives us a proof of FLT. *But note*: since three variables are involved, we must use what is called a "Gröbner basis" to determine divisibility — the standard single-variable long-division procedure is not applicable here.

Approach of Comparing Successive Inequalities

First Implementation of Approach

This Implemenation is being revised.

Second Implementation of Approach

1. By part (b) of "Lemma 1.5." on page 15, we know that

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

2. Now for all positive integers u and for all positive integers $k > 1$,

$u^k = u^{k-1} + u^{k-1}(u - 1)$.

Therefore we can write, from (1),

(2)
$x^p + y^{p-1} - z^{p-1} < x^{p-1} + x^{p-1}(x - 1)$.

And furthermore,

(3)
$x^p + y^p - z^{p-1} < x^{p-1} + x^{p-1}(x - 1) + y^{p-1}(y - 1)$.

And finally,

(4)
$x^p + y^p - z^p < x^{p-1} + x^{p-1}(x - 1) + y^{p-1}(y - 1) - z^{p-1}(z - 1)$, or,

by our assumption of the existence of a counterexample,

(5)
$0 < x^{p-1} + x^{p-1}(x - 1) + y^{p-1}(y - 1) - z^{p-1}(z - 1)$.

3. By "Lemma 1.0." on page 14, $x < y < z$. Let $y = x + b$, and $z = x + c$. Then it follows that:

$y - 1 = x + b - 1 = x - 1 + b, b > 0;$
$z - 1 = x + \mathrm{c} - 1 = x - 1 + c,\ 0 < b < c,$

and we can therefore write, from statement (5),

$0 < x^{p-1} + x^{p-1}(x - 1) + y^{p-1}(x - 1 + b) - z^{p-1}(x - 1 + c)$, or,

$0 < x^{p-1} + x^{p-1}(x - 1) + y^{p-1}(x - 1) + y^{p-1}b - z^{p-1}(x - 1) - z^{p-1}c$, or

(6)
$0 < x^{p-1} + (x - 1)(x^{p-1} + y^{p-1} - z^{p-1}) + y^{p-1}b - z^{p-1}c$.

4. By step 1, we can write, from (6):

(7)
$0 < x^{p-1} + (x-1)(< x^{p-1}) + y^{p-1}b - z^{p-1}c$, where "$< u$" denotes a number less than u.

Our goal now is to prove that the right-hand side of (7) is ≤ 0, thus giving us a contradiction that implies the truth of FLT.

5. Let us replace, unfavorably for our goal, "$(x-1)(< x^{p-1})$" with "$(x-1)(x^{p-1})$". Then (7) becomes

(8)
$0 < (x)x^{p-1} + y^{p-1}b - z^{p-1}c$.

Now, again unfavorably for our goal, let us replace "$y^{p-1}c$" *with* "$z^{p-1}c$". Then (8) becomes

$0 < (x)x^{p-1} + z^{p-1}((y-x) - (z - x))$, or

(9)
$0 < (x)x^{p-1} - z^{p-1}(z-y)$.

6. One way to determine if the right-hand side of (9) is 0 or negative is by considering the ratio

(10)

$$\frac{x^{p-1}x}{z^{p-1}(z-y)}$$

7. Since, by part (a) of "Lemma 1.5." on page 15 $x + y > z$, it follows that $z - y < x$. In fact, it is known[1] that $z - y$ can be as small as 1. If we can prove that

(11)

$$\frac{x^{p-1}x}{z^{p-1}}$$

[1] Ribenboim, Paulo, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, N.Y., 1970, p. 64.

is ≤ 1, then we will have a proof of FLT. A possible approach might be to prove that each of the $p - 1$ terms

$$\frac{x \cdot \ x^{1/(p-1)}}{z}$$

is ≤ 1 (recall that $x < y < z$) because then their product, which equals (11), will likewise by ≤ 1. The reader should keep in mind that, as of 1990, p was known to be > 125,000

Approach of Adding Inequalities

First Implementation of Approach

Suppose x, y, z are elements of a minimal counterexample $x^p + y^p = z^p$. By part (a) of "Lemma 1.5." on page 15, we know that, for all k, $1 \leq k \leq p - 1$, $x^k + y^k > z^k$, or, in other words, $x^k + y^k - z^k > 0$. We ask for the value of:

(1)
$S = (x^1 + y^1 - z^1\ ) + (x^2 + y^2 - z^2) + \ (x^3 + y^3 - z^3) + ... + (x^p\ + y^p - \ z^p\ ).$

By an elementary fact of algebra, we know that the value of (1) is given by:
(2)

$$S \ = \ \left(\frac{x^{p+1} - 1}{x - 1} - 1\right) + \left(\frac{y^{p+1} - 1}{y - 1} - 1\right) - \left(\frac{z^{p+1} - 1}{z - 1} - 1\right)$$

We ask if the assumption of a counterexample results in a value of (2) that is different from that in (1). in particular, we point out that

(3)
$S = (x^1 + y^1 - z^1\ ) + (x^2 + y^2 - z^2) + \ (x^3 + y^3 - z^3) + ... + (x^{p-1}\ + y^{p-1} - \ z^{p-1}\ )$

has the same value regardless if the assumed counterexample exists or not (because the exponent in the assumed counterexample is the smallest counterexample exponent).

Second Implementation of Approach

We now consider another implementation of the Approach of Adding Inequalities. Unfortunately, this implementation will not lead to a contradiction. It will lead only to the conclusion that the existence or non-existence of a counterexample has no effect on the value of (1), below. We begin by considering

$$\left(\frac{x^p-1}{x-1}\right)+\left(\frac{y^p-1}{y-1}\right)-\left(\frac{z^p-1}{z-1}\right)\quad -1$$

We can write the sum of the first three terms as
(1)

$$\frac{(x^p-1)(y-1)(z-1)+(y^p-1)(x-1)(z-1)-(z^p-1)(x-1)(y-1)}{(x-1)(y-1)(z-1)}$$

Since, by “Lemma 1.0.” on page 14, $p < x < y < z$, we know that:

$(x-1)(y-1) < (x-1)(z-1) < (y-1)(z-1)$. We can therefore “subtract out” $(x-1)(y-1)$ terms from the total number of (x^p-1) terms in the numerator of (1), and similarly for the (y^p-1) and (z^p-1) terms. By our assumption of a counterexample, the subtracted out terms taken together will become zero. Specifically, we have:

(2)
$(x^p-1)(y-1)(z-1) = \quad (x^p-1)((y-1)(z-1)-(x-1)(y-1)) + (x^p-1)(\ (x-1)(y-1);$
$(y^p-1)(x-1)(z-1) = \quad (y^p-1)((x-1)(z-1)-(x-1)(y-1)) + (y^p-1)(\ (x-1)(y-1);$
$-(z^p-1)(x-1)(y-1) = -(z^p-1)((x-1)(y-1)-(x-1)(y-1)) - (z^p-1)(\ (x-1)(y-1)).$
The sum of the rightmost terms in the three lines of (2) is
$x^p\ (x-1)(y-1) - (x-1)(y-1) +$
$y^p(x-1)(y-1) - \ (x-1)(y-1) -$
$z^p(x-1)(y-1) + (x-1)(y-1).$
By our assumption of a counterexample
$x^p\ (x-1)(y-1) +$
$y^p(x-1)(y-1) -$
$z^p(x-1)(y-1) =$
$(x^p + y^p - \ z^p)(x-1)(y-1) = 0 \cdot (x-1)(y-1) = 0.$

So the sum of the rightmost terms in the three lines of (2) = $-(x-1)(y-1)$.
The sum of the leftmost terms on the right-hand side of (2) is

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

Thus we have, for the value of (1),
(3)

$$\frac{(x^p-1)(y-1)(z-x)+(y^p-1)(x-1)(z-y)-\ (x-1)(y-1)}{(x-1)(y-1)(z-1)} =$$

(4)

$$\frac{(x^p-1)(y-1)(z-x)}{(x-1)(y-1)(z-1)}+\frac{(y^p-1)(x-1)(z-y)}{(x-1)(y-1)(z-1)}-\frac{(x-1)(y-1)}{(x-1)(y-1)(z-1)} =$$

$$\frac{(x^p-1)(y-1)(z-x)}{(x-1)(y-1)(z-1)}+\frac{(y^p-1)(x-1)(z-y)}{(x-1)(y-1)(z-1)}-\frac{(x-1)(y-1)}{(x-1)(y-1)(z-1)} =$$

(5)

$$\frac{(x^p-1)(z-x)}{(x-1)(z-1)}+\frac{(y^p-1)(z-y)}{(y-1)(z-1)}-\frac{1}{(z-1)}$$

Now $(z-x) = (z-1) - (x-1)$, and $(z-y) = (z-1) - (y-1)$, and so (5) equals

$$\frac{(x^p-1)(z-1)-(x^p-1)(x-1)}{(x-1)(z-1)}+\frac{(y^p-1)(z-1)-(y^p-1)(y-1)}{(y-1)(z-1)}-\frac{1}{(z-1)} =$$

$$\frac{(x^p-1)}{(x-1)}-\frac{(x^p-1)}{(z-1)}+\frac{(y^p-1)}{(y-1)}-\frac{(y^p-1)}{(z-1)}-\frac{1}{(z-1)} =$$

$$\frac{(x^p-1)}{(x-1)}+\frac{(y^p-1)}{(y-1)}-\frac{(x^p-1)}{z-1}-\frac{(y^p-1)}{z-1}-\frac{1}{(z-1)} =$$

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

$$\frac{(x^p - 1)}{(x - 1)} + \frac{(y^p - 1)}{(y - 1)} - \frac{(z^p - 1)}{z - 1}$$

which is exactly where we started. Our only conclusion can be that the existence or non-existence of a counterexample has no effect on the value of (1), which, to us at least, seems strange and worthy of further investigation.

Third Implementation of Approach

In this implementation, we proceed conceptually and informally, merely discussing an argument that could lead to a contradiction.

1. We begin by asking the reader to imagine a person who had never heard of FLT and who had never read this paper. The person is asked to describe a sequence of p fractions a_k/b_k, $1 \le k \le p$, p a large prime, having the properties:

(a) for each $k < p - 1$, $a_{k+1} > a_k$ and $b_{k+1} > b_k$;
(b) $a_p/b_p = 1$.

The person might respond with the following sequence or one like it:
(1)

$$\frac{1}{1}, \frac{2}{2}, \frac{3}{3}, \ldots, \frac{p}{p}$$

2. Suppose, now, that the person is told that the sequence must have the additional property that, for all $k < p$:

(c) a_k must be $> b_k$,

The person might then modify his or her sequence (1) to
(2)

$$\frac{2}{1}, \frac{3}{2}, \frac{4}{3}, \ldots, \frac{p}{p - 1}$$

3. Finally, suppose that the person is told that the sequence must have the further property that,
(d) for all $k < p$,

(3)

$$\frac{a_k}{b_k} > \frac{a_{k+1}}{b_{k+1}}$$

The person would rightly point out that his or her sequence in (2) already satisfies this property.

4. We observe that no fraction in (2) is equal to 1, although the limit of the value of the fractions as k approaches infinity is certainly 1.

5. By this time, the reader has probably understood that:

a_k corresponds to $x^k + y^k$;
b_k corresponds to z^k;
property (a) corresponds to the fact that
$x_{k+1} + y_{k+1}$ is always greater than $x_k + y_k$, and
z_{k+1} is always greater than z_k;
property (b) corresponds to our assumption that a counterexample exists;
property (c) corresponds to part (a) of "Lemma 1.5." on page 15;
property (d) corresponds to part (e) of "Lemma 1.5." on page 15.

6. In the series (2), we have, for all $k < p$, $a_{k+1} - a_k = 1$, *and* $b_{k+1} - b_k = 1$. In other words, the difference between successive a_k is constant, and similarly for the difference between successive b_k. We ask now what these differences are in the case of our assumption of a counterexample to FLT.

Clearly, for all positive integers u, k, $u^{k+1} - u^k = u^k(u - 1)$, and clearly this difference grows with increasing k, given fixed u. So, unlike the series (2), in the corresponding series for FLT, the difference between successive $x^k + y^k$ increases with increasing k, and similarly for the difference between successive z^k.

But this fact in itself does not necessarily have an impact on the difference $x^k + y^k - z^k$, as the reader can easily see from the following modification of the series (2), in which the difference between successive a_k increases by 1, and similarly for the difference between successive b_k.

(4)

$$\frac{2}{1}, \frac{4}{3}, \frac{7}{6}, \frac{11}{10}, \ldots, \frac{p}{p-1}$$

7. The reader should at this point recognize that the difference $x^k + y^k - z^k$ is of crucial impor-

tance for our approach. We draw the reader's attention to the fact that, by part (g) of "Lemma 1.5." on page 15, $x^k + y^k - z^k \geq (Kdef + k - 1)$, so that $(x^k + y^k)/z^k = (z^k + \geq (Kdef + k - 1))/z^k$, for $1 \leq k \leq p - 1$. Here, ("$\geq u$") denotes a quantity $\geq u$.

Approach by Induction on Inequalities

We begin by considering the following sequence *S* of inequalities, culminating in the assumed counterexample to the Theorem.

The Sequence S

The sequence *S* is:

$\{x^3 + y^3 \neq z^3,$

$x^4 + y^4 \neq z^4,$

$x^5 + y^5 \neq z^5,$

.

.

.

$x^{p\text{-}1} + y^{p\text{-}1} \neq z^{p\text{-}1},$

$x^p + y^p = z^p\}$

We can also express this sequence as a sequence of inner products:

$\{<x, y, z> \bullet <x^2, y^2, -z^2> = (x^3 + y^3 - z^3) \neq 0,$

$<x, y, z> \bullet <x^3 \ , y^3 , -z^3 > = (x^4 + y^4 - z^4) \neq 0,$

$<x, y, z> \bullet <x^4, y^4, - z^4 > = (x^5 + y^5 - z^5) \neq 0,$

.

.

.

$<x, y, z> \bullet <x^{p\text{-}2}, y^{p\text{-}2}, -z^{p\ \text{-}\ 2} > = (x^{p\text{-}1} + y^{p\text{-}1} -z^{p\text{-}1}) \neq 0,$

$<x, y, z> \bullet <x^{p\text{-}1}, y^{p\text{-}1}, -z^{p\text{-}1} > = (x^p + y^p -z^p) = 0\}$

The Basic Question

We now ask the Basic Question: *Is the sequence S possible?* In other words, could such a sequence of inequalities terminate in the indicated equality? Could we "get to" the indicated equality via the sequence of inequalities? We urge the reader to keep in mind that we are *not* merely attempting to approach FLT from the point of view of forms (homogeneous polynomials) of degree k, $1 \le k \le p$. A vast literature already exists on that approach. We are attempting to approach FLT from the point of view of the *sequence* of forms represented by S.

We now attempt to answer the Basic Question in the negative, considering first the sequence S from a factoring point of view, then considering the inner product representation of S.

The Sequence *S* Considered From a Factoring Point of View

Our assumption of a counterexample as the last item in the above list implies, by elementary algebra, that the sequence can be written:

$$\{x^3 \neq (z^3 - y^3 = (z - y)(z^2 + z^1y + y^2)),$$

$$x^4 \neq (z^4 - y^4 = (z - y)(z^3 + z^2y + zy^2 + y^3)),$$

$$x^5 \neq (z^5 - y^5 = (z - y)(z^4 + z^3y + z^2y^2 + zy^3 + y^4)),$$

...

$$x^{p-1} \neq (z^{p-1} - y^{p-1} = (z - y)(z^{p-2} + z^{p-3}y + \ldots + zy^{p-3} + y^{p-2})),$$

$$x^p = (z^p - y^p = (z - y)(z^{p-1} + z^{p-2}y + \ldots + zy^{p-2} + y^{p-1}))\ \}$$

Similar sequences exist with y^k, z^k on the left-hand side, $3 \le k \le p$.

We now prove two very elementary lemmas. Let:

$$(6)\quad \begin{aligned} B_{n,\,(z - y)} &= (z^{n-1} + z^{n-2}y + \ldots + zy^{n-2} + y^{n-1}). \\ B_{n,\,(z - x)} &= (z^{n-1} + z^{n-2}x + \ldots + zx^{n-2} + x^{n-1}). \\ B_{n,\,(x + y)} &= (x^{n-1} - x^{n-2}y + \ldots + y^{n-1}),\ n \ge 3. \end{aligned}$$

Lemma 20.0

If one of the following pairs,

(7) $((z - y),\ B_{r,\,(z - y)})$;
(8) $((z - x),\ B_{r,\,(z - x)})$;
(9) $((x + y),\ B_{r,\,(x + y)})$, r <u>a prime</u> ≥ 3.

has a factor in common, then that factor must be r.

Proof for the pair in (7):

1. Assume the pair in (7) have the prime q as a common factor.

2. Then $z - y = kq$ implies

(10) $z - y \equiv 0 \bmod q$,

and $B_{r, (z - y)} = mq$ implies

(11) $(B_{r, (z - y)} = (z^{r-1} + z^{r-2}y + ... + zy^{r-2} + y^{r-1})) \equiv 0 \bmod q$.

3. (10) implies $z \equiv y \bmod q$, so substituting y for z in (11) gives

(12) $ry^{r-1} \equiv 0 \bmod q$.

4.If $y \equiv 0 \bmod q$, then, by (10), $z \equiv 0 \bmod q$, contrary to (1.5). Therefore r must be $\equiv 0 \bmod q$. Since r is a prime, r must $= q$.

We leave it to the reader to verify that the proofs for (8) and (9) in the Lemma are similar. □

We now prove one more elementary lemma. I am indebted to Ivor Lloyd for bringing this lemma to my attention.

Lemma 28.0.
(a) *$(z – y)$ divides x^p, $(z – x)$ divides y^p, and $(x + y)$ divides z^p;*
(b) *$(z – y)$, $(z – x)$, and $(x + y))$ are co-prime in pairs. That is, $((z – y), (z – x)) = ((z – y), (x + y)) = ((z– x), (x + y))$* = 1.

Proof of Lemma 28.0 (a):
The reader can easily confirm that $(z – y)$ divides $(z^p – y^p)$, $(z – x)$ divides $(z^p – x^p)$ and $(x + y)$ divides $(x^p + y^p)$, since p is a prime greater than 2 (hence odd). But, on the assumption that a counterexample exists, $z^p – y^p = x^p$, $z^p – x^p = y^p$, and $x^p + y^p = z^p$. Therefore Part (a) is true.

Proof of Lemma 28.0 (b):
Since x, y, z are co-prime in pairs (by (1.5)), the result follows from Part (a). □

Observations

Keeping the Basic Question always before us, we now make the following observations.

(**A**) Since x, y, z are by hypothesis fixed, then so is the prime factorization of $(z - y)$, $(z - x)$, $(x + y)$.

(**B**) Therefore, if a counterexample exists, $(z - y)$ contains some of the prime factors of x^k, $(z - x)$ contains some of the prime factors of y^k, and $(x + y)$ contains some of the prime factors of z^k, for all $k \geq 2$.

(**C**) The process of constructing $B_{n, (z - y)} = (z^{n-1} + z^{n-2}y + ... + zy^{n-2} + y^{n-1})$ from $B_{n-1, (z - y)} =(z^{n-2} + z^{n-3}y + ... + zy^{n-3} + y^{n-2})$ is very simple: multiply through $B_{n-1, (z - y)}$ by z and add y^n. And similarly for $B_{n,\,(z\,-\,x)}$, and $B_{n,\,(x\,+\,y)}$.

If a counterexample exists, this process must yield $B_{p,\,(z\,-\,y)}$, which must contain all the prime factors of x not in $(z - y)$, and similarly for $B_{p,\,(z\,-\,x)}$, y, and $B_{p,\,(x\,+\,y)}$, z.

We remark in passing that:

$B_{n,\,(z\,-\,y)}$ can also be written $(z(...(z(z(z + y) + y^2) + y^3)...+ y^{n-1})$, and similarly for $B_{n,\,(z\,-\,x)}$, and $B_{n,\,(x\,+\,y)}$.

Furthermore, $B_{n,\,(z\,-\,y)}$ can also be written[1] $(x - \alpha_1 y)(x - \alpha_2 y)...(x - \alpha_{n-1} y)$, where $\alpha_{1,}\ \alpha_{2,\,...,}\ \alpha_{n-1}$ are the roots of $p(z) = z^{n-1} + z^{n-2} + ... + z + 1$ in the splitting field of $p(z)$. And similarly for $B_{n,\,(z\,-\,x)}$, and $B_{n,\,(x\,+\,y)}$.

Question 2. Recognizing that $B_{n,\,(z\,-\,y)}$, $B_{n,\,(z\,-\,x)}$ and $B_{n,\,(x\,+\,y)}$ are binary forms of degree $(n - 1)$, are there any results in the literature up to 1990, that enable us to prove that the process cannot yield such $B_{p,\,(z\,-\,y)}$, $B_{p,\,(z\,-\,x)}$, and $B_{p,\,(x\,+\,y)}$?

(**D**) There exists a prime r such that for all $r' > r$, $((z - y), B_{r'\,,\,(z\,-\,y)}) = ((z - x), B_{r'\,,\,(z\,-\,x)}) = ((x + y), B_{r'\,,\,(x+y)}) = 1$. Otherwise, by Lemma 20.0, x, y, z would each contain an infinite number of prime factors, an impossibility.

(**E**) By Lemma 20.0, if a counterexample exists, then we have the following possibilities:

(E.1) The exponent p does not divide either $(z - y)$ or $B_{p,\,(z\text{-}y)}$;
(E.2) The exponent p divides only $(z - y)$ but not $B_{p,\,(z\,-\,y)}$;
(E.3) The exponent p does not divide $(z -y)$ but divides $B_{p,\,(z\,-\,y)}$;
(E.4) The exponent p divides both $(z - y)$ and $B_{p,\,(z\,-\,y)}$.

And similarly for $((z - x), B_{r,\,(z\,-\,x)})$, and $((x + y), B_{r,\,(x\,+\,y)})$.

In other words, all prime factors of $(z - y)$ except for, possibly, p, and all prime factors of $B_{p,\,(z\,-\,y)}$ except for, possibly, p, are not only disjoint but are also pth powers. (If either or both terms $(z - y)$ and $B_{p,\,(z\,-\,y)}$ contain the prime p, then the combined power of p must $= p^p$.) The corresponding statement holds for $(z - x)$ and $(x + y)$. So if we were to embark on a "search" for counterexamples, x, y, z, we could immediately eliminate all those such that $(z - y)$, $(z - x)$, and $(x + y)$ failed to have prime factors conforming to these requirements.

Question 3: do any relevant results exist in the pre-1990 literature?

(**F**) Consider the sets

$G = \{ ..., 1/x^3, 1/x^2, 1/x, 1, x, x^2, x^3, ... \}$

and

[1] Borevich, Z. I., and Shafarevich, I. R., *Number Theory*, Academic Press, N.Y., 1966, p. 78.

$G' = \{ \ldots, 1/(\mathrm{B}_{3, (z - y)}), 1/(\mathrm{B}_{2, (z - y)}), 1, (z - y)\mathrm{B}_{2, (z - y)}, (z - y)\mathrm{B}_{3, (z - y)}, \ldots\}$

We ask: are G and G' infinite cyclic groups over the rationals, with:
x, $\mathrm{B}_{2, (z - y)}$ respectively as generators;
1 as the identity element in both cases;
multiplication/division by x the group operation of G;
multiplication/division of $\mathrm{B}_{n,(z - y)}$ by z and addition of y^n the group operation of G'.

If so, then they are isomorphic groups, by a well-known result. We now state a conjecture which, if true, implies the truth of FLT.

Conjecture 1.0[1]: There do not exist groups G, G' over the rationals having the following properties:
G, G' are infinite cyclic groups having generators g, g' where $g \neq g'$;
All elements of G, G' that are greater than the identity, 1, are positive integers;
For some exponent p and for no smaller exponent, $g^p = mg'^p$, where m is a fixed positive integer (it is equal to $(z - y)$ in our case);
For an infinite set of $k > p$, $g^k \neq mg'^k$.

(**G**) If we could prove that $\mathrm{B}_{p, (z - y)}$ cannot be a pth power, then we will have proved FLT for cases (E.1), (E.2), and (E.3) above. We observe that, if $m = z + y$, then:

$$m^{p-1} = (z+y)^{p-1} = \binom{p-1}{0}z^{p-1} + \binom{p-1}{1}z^{p-2}y + \ldots + \binom{p-1}{p-2}zy^{y-2} + \binom{p-1}{p-1}y^{p-1}$$

Now, by Pascal's triangle, we can see that $\mathrm{B}_{p, (z - y)}$ cannot be equal to m^{p-1}. Suppose we consider the set $T = \{m^n = (a + b)^n \mid m \geq 1, a, b, \geq 1, \ a + b = m, n \geq 1\}$, where $(a + b)^n$ is expanded as above in accordance with the binomial theorem, and suppose we imagine the elements of T as being organized in two lists, one by increasing m and then by increasing n, the other, say, lexicographically, by $(a + b)$. Then using these lists, we could find all possible occurrences of $\mathrm{B}_{n, (z - y)}$, including, specifically, $\mathrm{B}_{p, (z - y)}$.

Question 4: Can this strategy[2] enable us to prove that $\mathrm{B}_{p, (z - y)}$ can never be a pth power?
Note: there exists an infinity of binary forms of degree $n - 1$ which are, in fact, powers. For, if $a = b = n$, $n \geq 3$, then the binary form of degree n - 1, $a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1} = n \bullet n^{n-1} = n^n$. But this possibility is ruled out by the constraints on x, y, z, and n. Are there any other possibilities?

[1] I am indebted to J. D. Gilbey for correcting the statement of an earlier, more general version of this conjecture, and for then quickly disproving it. Gilbey did not see the current conjecture before this paper was placed on the web site.

Approaches Using the Calculus

First Vertical Approach Using the Calculus

1. The continuous function $f(k) = x^k + y^k - z^k$, $1 \le k \le p$, (see Figure 3) has the properties that $f(k)$ increases monotonically from an initial positive number to a maximum at $f(k')$, where $p - 1 < k' < p$, then decreases monotonically to 0 at $k = p$ ("Lemma 1.5." on page 15, and "On the Maximum of the Function f(k)" on page 53.

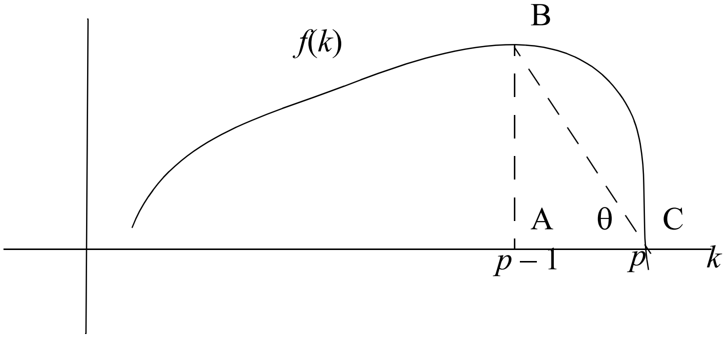

Fig. 3 Graph of the function $f(k)$

The maximum is greater than or equal to $Kdef + p - 2$, where $K = 2pU$, $U \ge 1$, each of d, e, f is greater than 1 ("Lemma 1.5." on page 15), and $p \ge 125{,}000$, by results established prior to Wiles' proof of FLT in the early nineties.

We remark in passing that the set of points $f(k)$ for integral k (including integral $k > p$) are the constituents of the congruence sets of elements $U(k, x, y, z) = x^k + y^k - z^k$, these sets being defined in the section "Discussion of the 4th Condition for the Truth of FLT' in Part (4) of this paper, on occampress.com.

2. Now for all $k \ge 1$,

$$(x^k + y^k - z^k) - (x^{k-1} + y^{k-1} - z^{k-1})$$

$$= (x^k - x^{k-1}) + (y^k - y^{k-1}) - (z^k - z^{k-1})$$

$$= x^{k-1}(x - 1) + y^{k-1}(y - 1) - z^{k-1}(z - 1). \qquad . \qquad (1)$$

Let $k = p$. Then (1) becomes

2. This strategy can be considered an application of the idea of "What = Where": *What* something is (e.g., its value) is a function of *where* it is in some structure — some database, as programmers might say. The most elementary example of the strategy is probably a binary tree. If we are asked to store the non-negative binary integers, then we can do so using a binary tree, in which, say, the digit 0 corresponds to descending the right-hand branch from a node, and the digit 1 corresponds to descending the left-hand branch from a node. Then the sequence of binary digits representing the integer is the address where the integer can be found in the tree: What =Where.

$$(x^p + y^p - z^p) - (x^{p-1} + y^{p-1} - z^{p-1})$$

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

or, by assumption that $x^p + y^p - z^p = 0$,

$$0 - (x^{p-1} + y^{p-1} - z^{p-1}) = x^{p-1}(x-1) + y^{p-1}(y-1) - z^{p-1}(z-1) \qquad (2)$$

Equation (2) seems a little surprising, for the following reason:

By "Lemma 1.5." on page 15, $x^{p-1} + y^{p-1} - z^{p-1}$ is a large positive number. Therefore $-(x^{p-1} + y^{p-1} - z^{p-1})$ is a large negative number.

We know that $p < x < y < z$ (by part (a) of "Lemma 1.0." on page 14); and that prior to Wiles' proof, p was known to be greater than 125,000. Therefore $(x-1)$ is very close to x, $(y-1)$ is very close to y, and $(z-1)$ is very close to z, so that $x^{p-1}(x-1) + y^{p-1}(y-1) - z^{p-1}(z-1)$ seems close to $(x^k + y^k - z^k)$, where k is slightly less than p (see Fig. 3). Therefore, by "Lemma 1.5." on page 15, it seems that $x^{p-1}(x-1) + y^{p-1}(y-1) - z^{p-1}(z-1)$ must be positive. And yet, by equation (2), it is in fact a large negative number.

With an eye on Fig. 3, we might be inclined to ask what power of x, $(x-1)$ is, and similarly for $(y-1)$ and $(z-1)$. We could then write $x^{p-1}(x-1) + y^{p-1}(y-1) - z^{p-1}(z-1) = x^{k'} + y^{k''} - z^{k'''}$, and then, since k', k'' and k''' are each less than p, we might be able to make an argument that $x^{k'} + y^{k''} - z^{k'''}$ is positive. Unfortunately, this will not work because it is impossible that $k' = k'' = k'''$. In fact, we have $k' < k'' < k'''$. The reason can be seen by comparing $log_{10}(10-1) \approx .954$, whereas $log_e(e-1) = ln(e-1) \approx (2.718-1) \approx 0.541$. We conclude that if $u < v$, and $u^h = (u-1)$, and $v^i = (v-1)$, then $h < i$. Thus it seems plausible that $x^{p-1}(x-1) + y^{p-1}(y-1) - z^{p-1}(z-1)$ is a negative number.

On the Maximum of the Function *f*(*k*)

By an elementary fact of the calculus, the derivative with respect to k of the function $f(k) = x^k + y^k - z^k$ is $f'(k) = x^k(ln\, x) + y^k(ln\, y) - z^k(ln\, z)$. Since $f(k)$ is continuous and smooth, and reaches a maximum at $k \geq (p-1)$ ("Lemma 1.5." on page 15), then descends monotonically to 0 at $k = p$ (see "Lemma 1.5." on page 15), it follows that there is a $k < p$ such that $f'(k) = x^k(ln\, x) + y^k(ln\, y) - z^k(ln\, z) = 0$. By definition of logarithm, this implies that

(1)

$$\frac{x^{x^k} y^{y^k}}{z^{z^k}} = 1$$

Since, by assumption, x, y, and z have no factors in common, that is, $(x, y) = (y, z) = (x, z) = 1$, we see that if k is an integer, in particular, if $k = p - 1$, the denominator cannot evenly divide the numerator, and thus (1) is contradicted. So we have proved that the maximum of $f(k)$ occurs at some k where $p - 1 < k < p$.

Second Vertical Approach Using the Calculus

1. As we stated in the previous sub-section, the derivative of $f(k)$, $f'(k)$, is $x^k(ln\ x) + y^k(ln\ y) - z^k(ln\ z)$. See Fig. 3: by the mean value theorem, it is clear that there exists a k'', where $p - 1 < k'' < p$, such that

(1)
$f'(k'') = x^{k''}(ln\ x) + y^{k''}(ln\ y) - z^{k''}(ln\ z) = (x^{p-1} + y^{p-1} - z^{p-1})/1$, where the right-hand side of the equation is *tan* θ.

2. Now the right-hand side of (1) is clearly an integer. If we can show that the left-hand side is not an integer, then we will have a proof of FLT.

Since the natural logarithm of an integer is irrational, we know that *ln x*, *ln y* and *ln z* are each irrational. Clearly k'' lies between $p - 1$ and k, so $x^{k''}$, $y^{k''}$, and $z^{k''}$ are not integers. Clearly the sum of no two of the three terms on the left-hand side = 0. Since, by definition, no irrational number has an infinitely repeating cycle in the digits of its decimal expansion, and an integer, on the other hand, being rational, does have such an infinitely repeating cycle, and furthermore, that cycle consists solely of 0s, it is tempting to be optimistic that the left-hand side of (2) is irrational, or at least not an integer.

However, we saw in the previous sub-section that $f'(k) = x^k(ln\ x) + y^k(ln\ y) - z^k(ln\ z) = 0$. That is, a left-hand side, which we might have been tempted to say was irrational, turns out to be equal to an integer, namely, 0. In fact, let a, b, c be any positive integers such that $ab = c$. Then $ab/c = 1$. Taking the natural logarithm of each side of this last equation, we get $ln(ab/c) = ln(1)$, or $ln(a) + ln(b) - ln(c) = 0$. So even though each of the three terms on the left-hand side are irrational, the right-hand side is an integer.

Furthermore, since $f'(k)$ is continuous, and has a derivative, it is clear that $f'(k)$ ranges continuously from $f'(k) = 0$ to a large negative value at $f'(p)$. Therefore, during this transition, $f'(k)$ necessarily passes through a large number of integer values.

We tentatively conclude that this Approach is without promise.

Approach via Factors of *x*, *y*, *z*

1. If a counterexample $x^p + y^p = z^p$ exists, then
(a) $x^p = z^p - y^p$;
(b) $y^p = z^p - x^p$;
(c) $z^p = x^p + y^p$.

By an elementary fact of algebra, (a), (b), (c) imply

(a′) $x^p = z^p - y^p = (z - y)(z^{p-1} + z^{p-2}y + z^{p-3}y^2 + ... + y^{p-1})$;
(b′) $y^p = z^p - x^p = (z - x)(z^{p-1} + z^{p-2}x + z^{p-3}x^2 + ... + x^{p-1})$;
(c′) $z^p = x^p + y^p = (x + y)(x^{p-1} - x^{p-2}y + x^{p-3}y^2 - ... + y^{p-1})$;
respectively.

(a′), (b′), (c′) imply

(a″) x and $(z-y)$ have a factor ≥ 1 in common, i.e., $(x, z-y) = d$, where $d \geq 1$;[1]
(b″) y and $(z-x)$ have a factor greater than 1 in common, i.e., $(y, z-x) = e$, where $e > 1$;
(c″) z and $(x+y)$ have a factor greater than 1 in common, i.e., $(z, x+\mathrm{y}) = f$, where $f > 1$;
respectively.

From (a″), (b″), and (c″) it follows that

(a‴) x and $(z-y)$ are both multiples of d, or,
$x \equiv 0 \bmod d$,
$z-y \equiv 0 \bmod d$,
hence $x \equiv\ z-y \bmod d$;

(b‴) y and $(z-x)$ are both multiples of e, or,
$y \equiv 0 \bmod e$,
$z-x \equiv 0 \bmod e$,
hence $y \equiv\ z-x \bmod e$;

(c‴) z and $(x+y)$ are both multiples of f, or,
$z \equiv 0 \bmod f$,
$x+y \equiv 0 \bmod f$,
hence $z \equiv\ x+y \bmod f$;
respectively.

From (a‴), (b‴), and (c‴) it follows that
(a⁗) $x+y-z \equiv 0 \bmod d$,
(b⁗) $x+y-z \equiv 0 \bmod e$,
(c⁗) $x+y-z \equiv 0 \bmod f$,
respectively.

Therefore we can conclude that $x+y-z$ is a multiple of the least common multiple of *d, e, f* (*[d, e, f]*). Since, by statement (1.5) under "Initial Assumptions, Definitions, and Properties of Numbers Involved" on page 12, $(x, y) = (y, z) = (x, z) = 1$, we know that ($d$, e, f) must = 1, because otherwise, two of x, y, z must have a factor in common.

But then, by a fundamental fact of elementary number theory, [d, e, f] must equal *def.* Thus $x+y-z = Kdef$, *where* $K\ \geq 1$.

Is there a basis for a proof of FLT in these facts?

[1] Since it is possible that $z-y = 1$ (Ribenboim, Paulo, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, N.Y., 1970, p. 64).

Approach Using *x* = *z* - *h*, *y* = *z* - *k*

Preliminaries

Assume a minimum counterexample exists, and let $x = z - h$, $y = z - k$. Then

1. $(z - h)^p + (z - k)^p = z^p$.

2. By the binomial theorem, this equation implies

$z^p - A + z^p - B = z^p$, *or* $-z^p = -A - B$.

3. By the binomial theorem, since p is an odd prime,
(1)

$$-A = -\binom{p}{1}z^{p-1}h + \binom{p}{2}z^{p-2}h^2 - \binom{p}{3}z^{p-3}h^3 + \ldots - h^p$$

$$-B = -\binom{p}{1}z^{p-1}k + \binom{p}{2}z^{p-2}k^2 - \binom{p}{3}z^{p-3}k^3 + \ldots - k^p$$

Adding $-A$ and $-B$ and gathering terms, we have

(1)

$$-A - B = -\binom{p}{1}z^{p-1}(h+k) + \binom{p}{2}z^{p-2}(h^2+k^2) - \binom{p}{3}z^{p-3}(h^3+k^3) + \ldots - (h^p + k^p)$$

4. We now assert that $h + k < z$.

Proof:

By step 1, we have $x = z - h$, $y = z - k$. By "Lemma 0.0" on page 13, we know that $x + y > z$. Therefore $z - h + z - k. > z$, or $h + k < z$. □

5. Next, we assert that $h^i + k^i < z^i$, where $1 \le i < p$.

Proof:

From step 4 we have $h + k < z$. Therefore $(h + k)^i < z^i$, from which it surely follows, by the binomial theorem, that $h^i + k^i < z^i$. □

6. And next, we assert that $x^i + y^i > z^i$, where $1 \le i < p$.

Proof: See "Lemma 1.5, Statement and Proof", in Part (2) of this paper, on occampress.com.

First Implementation of Approach

1. We write, from (0) in the "Preliminaries" sub-section, $-A = -A' - h^p$ and $-B = -B' - k^p$. In other words, $-A'$ is all of $-A$ except for the last term, and similarly for $-B'$.

Thus we can write the first equation in step 2 of the "Preliminaries" sub-section, as

(1)
$z^p - A' - h^p + z^p - B' - k^p = z^p$

2. Now since by definition at the start of "Preliminaries", $x = z - h$ and $y = z - k$, we have $h = z - x$ and $k = z - y$. Substituting into (1) in this sub-section we have

$z^p - A' - (z - x)^p + z^p - B' - (z - k)^p = z^p$

By the binomial theorem, this implies

$z^p - A' - z^p + C' + x^p + z^p - B' - z^p + D' + y^p = z^p$

3. Recalling that, by assumption of a counterexample, $x^p + y^p = z^p$, and cancelling z^p's, we have

$-A' + C' - B' + D' = 0$, or

(2)
$C' + D' = A' + B'$.

4. But, by step 3 in the "Preliminaries" sub-section,

$$C' + D' = \sum_{i=1}^{p-1} (-1)^i \binom{p}{i} z^{p-i} (x^i + y^i)$$

and

$$A' + B' = \sum_{i=1}^{p-1} (-1)^i \binom{p}{i} z^{p-i} (h^i + k^i)$$

5. By step 6 in the "Preliminaries" sub-section, $x^i + y^i > z^i$, and by step 5 in the same sub- section, $h^i + k^i < z^i$, and so each *positive* term in $C' + D'$ is *greater than* the corresponding *positive* term in $A' + B'$. But each *negative* term in $C' + D'$ is *less than* (more negative than) the corresponding *negative* term in $A' + B'$. If we can show that these facts make (2) false, then we will have a proof of FLT. However, that will require showing that the greater positive terms in $C' + D'$ are not somehow "cancelled" by the greater native terms in $C' + D'$.

Second Implementation of Approach

By the equation in step 2 of the sub-section "Preliminaries", in order to avoid a contradiction, we must have $-z^p = -A - B$. We attempt to show that the right-hand side of (1), in step 3 of "Preliminaries", is greater than z^p. If we can show this, then we have a proof of FLT.

Our attempt will be aided if it is true that, for all i, $2 \le i \le p$,

(1)

$$(z^{p-1})\left|\binom{p}{1}(h^1 + k^1)\right| > (z^{p-2})\left|\binom{p}{2}(h^2 + k^2)\right| > \ldots > (z^{p-i})\left|\binom{p}{i}(h^i + k^i)\right| > \ldots > \left|\binom{p}{p}(h^p + k^p)\right|$$

If (1), here, is true, then we might be able to reason (informally) as follows. The first term in (1) in the sub-section "Preliminaries" is negative. However, (1) in that sub-section must equal, not merely zero, but $-z^p$. The second term in (1) in the sub-section "Preliminaries" is positive, but if (1) above in this sub-section is true, it is not sufficiently positive to be greater than or equal to the first term. The third term in (1) in the sub-section "Preliminaries" is negative and so only increases the net negative value so far. The fourth term is positive but is not sufficiently positive to be greater than or equal to the net negative value so far. Etc.

Since $p < x < y < z$ (by part (a) of "Lemma 1.0." on page 14), so that $p < z$, and since it appears that $(h^i + k^i)$ falls rapidly below z^i as i increases, there is reason to believe that (1) in this sub-section is true.

As far as the rate at which $(h^i + k^i)$ falls is concerned, assume, as a worst case, and contrary to fact, that $h + k = z$ (actually, $h + k < z$). Then $h^i + k^i = z^i - U_i$, where U_i is the sum of all the terms of the binomial expansion of $(h + k)^i$ except for the first and the last that is, except for $h^i + k^i$. Then we are trying to show that

$$(z^{p-i})\left|\binom{p}{i}(z^i - U_i)\right| > (z^{p-(i+1)})\left|\binom{p}{i+1}(z^{i+1} - U_{i+1})\right|$$

for all relevant *i*, or
(2)

$$\binom{p}{i}z^p - \binom{p}{i}z^{p-i}U_i > \binom{p}{i+1}z^p - \binom{p}{i+1}z^{p-(i+1)}U_{i+1}$$

Now, the sequence of binomial coefficients in Pascal’s triangle is symmetrical, increasing only for the first $(p - 1)/2$ coefficients, and so these initial coefficients are the only ones we need be concerned with. The first term on the right-hand side of the inequality in (2) is less than *p* times the first term on the left-hand side. The question is, Is the second term on the right sufficiently more negative than the second term on the left that it can overcome the increase in the positive value of the first term on the right, in addition to being more negative than the second term on the left? If the answer is yes, then we have our desired result. This question is in part the question, Do the non-*z* factors in the second term on the right, overcome the loss of one *z* factor in the second term on the right?

“Computational” Approaches

By a “computational approach” to a proof of FLT, we mean one that either utilizes the computer directly, or else one that is based on programming or computer science concepts. Following are three such approaches.

In the first approach we convert the question of the truth of FLT to a question about the correctness of a program. In the second approach, we compare, step by step, the computation of $x^p + y^p$ vs. the computation of z^p and attempt to show that the computations cannot produce the same value. The third approach is based on an idea from algorithmic information theory.

Can We Find Out If Fermat Was Right After All?

We believe that the day is not far off when it will be possible to supply a computer program with what scholars believe was Fermat’s mathematical knowledge at any specified time in his career, and then give the computer a proof of FLT as a goal and ask it to return all possible attempts at a proof of length 1 step, then all possible attempts at a proof of length 2 steps, etc. Ideally, the program would be interactive, so that the researcher could make suggestions as to how to go about finding such a proof. Of course, an immediate question is, What constitutes a “step” in this context? As every student of mathematics knows, a complicated proof — i.e., one that requires many steps — is often broken down into a “simpler” proof in which steps are grouped into supersteps. Or, putting it another way (see William Curtis’ *How to Improve Your Math Grades* on the web site www.occampress.com), it is possible to approach a proof in a top-down fashion, in which, at the top-most level, there are only a few steps, each being the equivalent of a lemma or theorem. If all the lemmas or theorems are valid, then the proof is valid. The proof of each lemma or theorem is then proved, recursively, in the same fashion.

In the case of FLT, the user might set up sequences of statements, each sequence constituting the top level of a possible proof, e.g., a proof by induction, then see if the program can find a proof of each statement.

Approach by a Certain Class of Program

In our paper, "Occam's Razor and Program Proof by Test" (www.occampress.com), a Class of algorithms is defined having the property that whether or not the algorithms compute the same function can be decided in a known finite number of tests. In brief, the Class is defined as follows (p. 17):

Let p be a program in the Class, and let p consist of x instructions, $x \geq 1$, under some appropriate Turing machine formalism. Then

> each instruction is executed at least once in the computation of all strings of length $x + 1$, and
> each instruction is executed at least once in the computation of all strings of length $x + 2$, and
> each instruction is executed at least once in the computation of all strings of length $x + 3$, and
> ...

It might be possible to prove the Theorem as follows. Create a program $p_1(x, y, z, n)$ that computes $x^n + y^n - z^n$. If the result is not 0, then the program returns a 1, otherwise it returns a 0. Create another program $p_2(x, y, z, n)$ that returns 1 for all inputs x, y, z, n. Now if these programs are in the Desired Class, it should be possible, in a finite number of tests, to determine if the programs p_1 and p_2 both compute the same function, namely, the function which returns 1 for all inputs x, y, z, n. If the programs both compute this function, then we have a proof of Fermat's Last Theorem.

Approach by "The Extra +"

Description of Approach

A programmer looking at the two sides of the FLT inequality $x^n + y^n \neq z^n$ might see that the two sides can be computed by the same program, call it P. In other words, for each triple $<x, y, n>$ a copy of the program P returns the value $x^n + y^n$, and for the triple $<z, 0, n>$ a copy of the program P returns the value of $z^n + 0^n$ $(= z^n)$. Furthermore, the programmer would see that we can run the computation of the left-hand and right-hand sides "in unison", with incrementation (by 1) being the basic computational operation. (Exponentiation is repeated multiplication, multiplication is repeated addition, and addition is repeated incrementation-by-1 as implemented by a subprogram called, say, *incr*.) By "in unison" we mean that each execution of *incr* during the course of computing the left-hand side, takes place at the same time as each execution of *incr* on the right-hand side.

We implement P as a Turing machine. We denote the copy of P that computes the left-hand side of the inequality as P_L, and the copy that computes the right-hand side as P_R. Without loss of generality, we require that P, hence both copies, have a single input tape, a single work tape, and a single output tape. At the start of its computation, P_L's input tape contains x, y, n; P_R's input tape contains z, 0, n.

A counter C_L is present in P_L, and a counter C_R is present in P_R. Both are set to 0 when P_L and P_R start computing. C_L counts the number of successive invocations of *incr* that occur when P_L performs its computation. Similarly, C_R counts the the number of successive invocations of *incr* that occur when P_R performs its computation.

When P_L has completed the computation of x^n and y^n, it copies x^n to the output tape, and then proceeds to, in repeated succession, decrement y^n on the work tape and to increment the contents of the output tape (x^n + ...) until y^n is 0, whereupon P_L halts. Similarly, when P_R has completed the computation of z^n and 0^n (nothing to compute in the latter case, of course), it copies z^n to its output tape, and then proceeds to decrement 0^n on the work tape. But there is nothing to decrement, and so P_R halts.

Assume, now, that FLT is false, or, in other words, that for some $x, y, z, n = p$ as described above under "Initial Assumptions, Definitions, and Properties of Numbers Involved" on page 12, $x^p + y^p = z^p$. Then after P_R has computed $z^p + 0^p$, the counter C_R will show z^p incrementations. But after P_L has completed execution of x^p and y^p, the counter C_L will likewise show (by hypothesis) a total of z^p incrementations. *But P_L has not finished executing!* It must add x^p and y^p (this is the "extra +" in the title of this sub-section), and this will cause C_L to show a total count greater than z^p by the time P_R completes computation of $x^p + y^p$. Thus, contrary to hypothesis, and in conformity with fact (ever since Wiles' proof of FLT) $x^p + y^p \neq z^p$.

Discussion of Approach

It has been argued[1] that the above Approach must include an explanation why the Approach doesn't prove that there are no positive integers x, y, z such that $x + y = z$, or $x^2 + y^2 = z^2$, which, of course, is contrary to fact.

The explanation is that, by Lemmas 0.0 and 0.5, there are no such x, y, z that can be a counterexample to FLT, and the Approach is based on the assumption that x, y, z are elements of such a counterexample! In other words, if the Approach is applied to <x, y, 1>, and <z, 0, 1>, or to <x, y, 2>, and <z, 0, 2>, the counters are guaranteed to contain different counts at the end of each computation.

In passing, we must remind the reader that, for a proof-by-contradiction of the proposition **r**, all we need to do is to assume not-**r**, and from that assumption, arrive at a contradiction. The proposition **r** is then proved (if, with most mathematicians, we accept the validity of proof-by-contradiction). We are not required to explain why the argument used in the proof does not work in another context (for example, the context in which x, y, z are not elements of a counterexample). Of course, readers may attempt to find a flaw in the argument by applying it to other contexts. That is perfectly legitimate. But then they must come back to the original argument and show where it is faulty.

However, we must confess that the argument presented in "Description of Approach" on page 60 has failed to convince readers. Some do not accept what we say at the start of this sub-section regarding the cases for the exponents 1 and 2. But no reader, so far, has pointed to the first sentence in "Description" that he or she believes is wrong. At the very least, then, we feel we should try to justify our intuition, which began with the question, Why is it that no program that computes $a^k + b^k$, can ever compute a c^k that has the same value, for any a, b, c, and for $k > 2$?

[1] by Monsur Hossain

Naively, our answer was "that extra +" that is needed to make $a^k + b^k = c^k$. On the right-hand side, all that the program needs to do is compute *ccc...c* (*k c*'s). On the left-hand side it needs to compute *aaa...a* (*k a*'s), then it needs to compute *bbb...b* (*k b*'s), then add the two results together. No wonder (we felt) the two sides can never be equal!

We tried to make our intuition concrete by reducing the computation of each side to incrementations by 1, which can be done if we represent the program that computes both sides as a Turing machine, and by requiring the computation of each side to proceed in unison.

At present, our first question to readers who reject our argument is, How would you tally the number of incrementations that occur during the computation of each side if not in the way we have described? So far, we have not received an answer.

.Before leaving this Approach, we should also consider a possible application of the "*Vertical Approach*" (see "Brief Summary of Approaches Described in This Paper" on page 9) to the use of programs in a possible proof of FLT. That is, we should inquire into the behavior of a *program* that successively computed, for *x*, *y*, *z* of a counterexample,

$x^3 + y^3$, and z^3, and found them to be unequal,
$x^4 + y^4$, and z^4, and found them to be unequal,
...
$x^{p-1} + y^{p-1}$, and z^{p-1}, and found them be unequal,
$x^p + y^p$, and z^p, and found them to be *equal*.

Approach by Algorithmic Information Theory

A fundamental concept in algorithmic information theory is that of the minimal length program to compute a given number *n* (or a given function *f*), i.e., the program (or programs) whose length *l* in number of symbols, $l \geq 1$, is the minimum for all programs that compute the number *n* (or the function *f*).

If we can show that the minimum length of a program that computes $x^p + y^p$ must always be different from the minimal length of a program that computes z^p, we will have a proof of FLT.

Superficially, such a proof seems obtainable, since we can derive from the above program *P* a shorter program *P′* to compute z^p by simply removing the second while loop from *P*. But there is nothing in the minimal length property that requires that a given number or function be computed "nicely", e.g., the way a competent programmer would write a program to compute the number or function. Any sequence of machine-executable instructions that yields the desired number, no matter how bizarre the sequence, is by definition a program that computes the number or function. So, further investigation is required to see if this Approach holds any promise.

n-Dimensional Geometric Approaches

We begin by asking the question, "Is there a Pythagorean theorem in dimensions greater than 2?"

Our answer is a qualified yes. Here is our reasoning:

1. Any two straight lines of non-zero finite length can be the legs of a right triangle.

2. The Pythagorean theorem applies to all right triangles.

3. Let *a, b* be any positive integers, and *k* a positive integer, where $3 \leq k$.

Then $a^{k/2}$ and $b^{k/2}$ can be the legs of a right triangle. Therefore, by the Pythagorean theorem,

(1)

$$(a^{k/2})^2 + (b^{k/2})^2 = c^2$$

Let $c = d^{k/2}$, where *d* is a real number, not necessarily an integer, or even a rational. Clearly, $d = c^{2/k}$. So, from (1) we have

(2)

$$(a^{k/2})^2 + (b^{k/2})^2 = (d^{k/2})^2$$

and thus

(3)

$$a^k + b^k = d^k$$

The above argument is recent. The preceding reasoning was as follows:

We ask, "Is there a 'Pythagorean theorem' in three dimensions, and if not, why not?" We observe that there is most certainly a "Pythagorean theorem" in one dimension: on the real line, simply mark three different points *a*, *b*, *c*. Then the distance *ab* + the distance *bc* = the distance *ac*.

As we know, there is a Pythagorean theorem in two dimensions: in the plane, form a right triangle with vertices *a*, *b*, *c*, where *ac* is the hypotenuse. Then the (area of the) square on the side *ab* + the (area of the) square on the side *bc* = the (area of the) square on the side *ac*.

Now let us see if there is a "3-dimensional right triangle" to which a 3-dimensional Pythagorean theorem might apply. Fig. 4 shows what we will call a "3-dimensional right triangle".

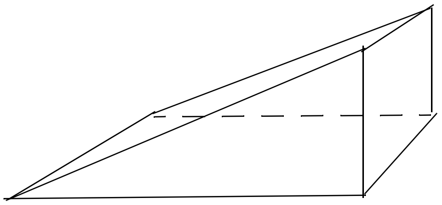

Fig. 4 A "3-dimensional right triangle"

We ask if it can be the case that, for such a "right triangle", the (volume of the) cube on one side + (the volume of the) cube on another side = (the volume of the) cube on the "hypotenuse side"? The reader can easily convince him- or herself that the answer is always no: all three of the (planar) sides of the "3-dimensional right triangle" cannot be squares, hence cannot be faces of cubes. It would be nice if this fact implied that there do not exist x, y, z such that $x^3 + y^3 = z^3$, but unfortunately it does not. The reason is this:

We have established that:

If x and y are the legs of a right-triangle and z is the hypotenuse (implying that $x^2 + y^2 = z^2$) then $x^3 + y^3 \neq z^3$.

The contrapositive of this statement is:

If $x^3 + y^3 = z^3$, then it is not the case that (x and y are the legs of a right-triangle and z is the hypotenuse …)

In other words, a counterexample is still possible as long as x, y, z are not the sides and hypotenuse of a right-triangle.

Thus, we are not encouraged to wonder if n-dimenstional right triangles also do not exist, where $n > 3$, and, if they do not, to wonder if that implies the truth of FLT.

Of course, we do not need right triangles to prove that, at least in the case of the integers, there exist a, b, c such that $a^2 + b^2 = c^2$. For it is well-known that if r, s are any integers, and if $a = r^2 - s^2$, $b = 2rs$, and $c = r^2 + s^2$, then $a^2 + b^2 = c^2$. So we can wonder if there are geometrical arguments not involving "triangles" to show why, for no x, y, z is it the case that $x^3 + y^3 = z^3$.

An obvious place to begin is to assume that we have a countable infinity of n-by-n cubic boxes, where $n \geq 1$. In addition, we have a countable infinity of unit cubes. Each box contains exactly n^3 of these cubes. Assume that there exists a box with side x, another box with side y, and a third box with side z, and that the number of cubes in the x box, plus the number of cubes in the y box = the number of cubes in the z box.

Next, assume there is a duplicate box with side z, but that it is empty. We are now going to attempt to fill it with the cubes from the x and y boxes. We will do this one layer at a time, a layer being one unit-cube thick and measuring z by z cubes — thus, containing z^2 unit cubes.

We ask how many layers we will get from the x box. The answer is

$$\frac{x^3}{z^2} = q_x + \frac{r_x}{z^2}$$

where $r_x < z^2$.

Similarly, the number of layers we will get from the y box will be

$$\frac{y^3}{z^2} = q_y + \frac{r_y}{z^2}$$

where $r_y < z^2$.

Then, in order for our assumption that $x^3 + y^3 = z^3$ to be true, it must be the case that

$$\left(\frac{x^3}{z^2} + \frac{y^3}{z^2}\right) z^2 = z^3$$

The term in parentheses equals z. Since $x < y < z$, $x^3/z^2 < x$ and $y^3/z^2 < y$. Unfortunately, we seem to have run up against a problem of too little information to proceed further.

Appendix A — Lemma 3.0

The proof of this lemma is now in Part (2) of this paper on the web site occampress.com.

Appendix B

Contents of this Appendix have been moved to "First Vertical Approach Using the Calculus" on page 52.

Appendix C

Contents of this Appendix have been moved to "Another Approach" on page 23 in the section "Vertical Approaches Based on Congruences" on page 21.

Appendix D — Proof of Lemma 6.0

The proof of this Lemma is now in Part (2) of this paper, on the web site occampress.com.

Appendix E — Summary of Results Used in Strategies

Assumptions

We assume there exist x, y, z such that, for some prime p, $x^p + y^p = z^p$. If FLT is true for p, then it is true for all multiples of p ("Lemma 0.6" on page 14).

We assume that p is the minimum such p.

Without loss of generality we assume that $(x, y) = (y, z) = (x, z) = 1$. In this case, trivially, exactly one of x, y, z is even.

Table of Results

Table 1: Summary of Results Used in Strategies

Result	Reference
$x + y > z$.	Part (a) of "Lemma 1.5." on page 15
If $x^2 + y^2 = z^2$, *then x, y, z cannot be elements of a counterexample.*	Part (a) of "Lemma 1.5." on page 15
For all k, $1 \le k \le (p-1)$, $x^k + y^k > z^k$.	Part (a) of "Lemma 1.5." on page 15
For all k, $1 \le k < p$, $$\frac{x^k + y^k}{z^k} > \frac{x^{k+1} + y^{k+1}}{z^{k+1}}$$	Part (e) of "Lemma 1.5." on page 15
For all $k > p$, $x^k + y^k < z^k$.	"Lemma 1.95." on page 15
$p < x < y < z$.	"Lemma 1.0." on page 14
$p > 125{,}000$ *(as of 1990).*	Ribenboim, Paulo, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, N.Y., 1970, p. 199.
$z < 2y$.	"Lemma 2.0" on page 16
$z < x^2$.	"Lemma 2.5" on page 16
y, z, have at least two prime factors.	Ribenboim, Paulo, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, N.Y., 1970, p. 64.

Table 1: Summary of Results Used in Strategies

Result	Reference
If x is prime, then $z - y = 1$.	ibid., p. 64
For given x, y, z such that $x^p + y^p = z^p$, p can be at most one prime.	“Lemma 4.0.5” on page 16
For p such that, for some x, y, z, $x^p + y^p = z^p$, it is possible that there exists x', y', z' such that $x'^p + y'^p = z'^p$. (In this case, we can define a “minimum” counterexample as follows: choose x', y', z' having minimum x'. If there is more than one such x', y', z', choose the one having minimum y'. (It is not possible for there to be more than one z' in that case.))	Ribenboim, Paulo, *13 Lectures on Fermat’s Last Theorem*, Springer-Verlag, N.Y., 1970, p. 232.
If $(x, m) = (y, m) = (z, m) = 1$ and *$x \equiv u \bmod m$, and $y \equiv v \bmod m$, and $z \equiv w \bmod m$, then* *if $x^r + y^r \equiv z^r \bmod m$, $r \geq 1$,* *then $u^r + v^r \equiv w^r \bmod m$.*	(1.91(c)) in Part (2) of this paper, on the web site www.occampress.com
There exists a prime q such that at least one of $x, y, z > q$.	“Appendix D — Proof of Lemma 6.0” in Part (2) of this paper, on the web site occampress.com.
Let p be an odd prime, and let t be a positive integer. Then there exists an infinity of odd primes q such that $(p, q - 1) = (t, q - 1) = 1$.	“Lemma 3.0: Statement and Proof” in Part (2) of this paper on occampress.com
$((z - y), (z - x), (x + y)) = 1$, i.e., *the three terms do not have a factor in common*.	“” on page 49
$$\lim_{k \to \infty} \frac{x^k + y^k}{z^k} = 0$$	“Lemma 1.97” on page 15

Table 1: Summary of Results Used in Strategies

Result	Reference
Let: $B_{n, (z - y)} = (z^{n-1} + z^{n-2}y + ... + zy^{n-2} + y^{n-1})$. $B_{n, (z - x)} = (z^{n-1} + z^{n-2}x + ... + zx^{n-2} + x^{n-1})$. $B_{n, (x + y)} = (x^{n-1} - x^{n-2}y + ... + y^{n-1}), n \geq 3$. *Then if one of the following pairs,* (7) $((z - y), B_{r, (z - y)})$; (8) $((z - x), B_{r, (z - x)})$; (9) $((x + y), B_{r, (x + y)})$, *r a prime* ≥ 3, *has a factor in common, then that factor must be r.*	"Lemma 20.0" on page 48

Appendix F — Statement and Proof of Certain Numbered Statements and of Lemmas

This Appendix is now in Part (2) of this paper, on the web site occampress.com.

Bibliography

Borevich, Z. I., and Shafarevich, I. R., *Number Theory*, Academic Press, N.Y., 1966, pp. 156-164.

Edwards, Harold M., *Fermat's Last Theorem*, Springer-Verlag, N.Y., 1977.

Ribenboim, Paulo, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, N.Y., 1979.