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@cs.com
Phone: (510) 548-3827

Aug. 19, 2011

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?" Probably our most promising approach is what we call the "Vertical" approach. Here, instead of trying to expand the set of exponents n for which FLT is true, as had been traditionally done, we attempt to expand the set of ordered triples $<x, y, z>$ for which FLT is true for all exponents n. For example, for assumed counterexample $x^p + y^p = z^p$ we study the sequence $x + y \neq z$, $x^2 + y^2 \neq z^2$, $x^3 + y^3 \neq z^3$, ..., $x^p + y^p = z^p$ with the aim of deriving a contradiction. We also study several approaches utilizing ideas from computer science.

Key words: Fermat's Last Theorem

Statement of the Theorem and Brief History

Fermat's Last Theorem (FLT) states that:

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

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) 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.)[1] 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?

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 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

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

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)

Despite the above skepticism, we believe that some of the approaches to a proof of FLT that are set forth in this paper were well within reach of Fermat.

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 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. More details are given below under ""Vertical" Approaches" on page 7.

- 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 now or 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 50.

• 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 50.

• 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 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.

• "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 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 Implementations of Approaches to a Proof of FLT, in Our Opinion" on page 10, 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 one of the most important of our approaches to a proof, namely, the approach based on the "lines-and-circles" model of congruence.

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

Proofs 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.

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
  - Vertical Approaches Based on Congruences
  - Vertical Approaches by Induction on Inequalities
  - Vertical Approach Using the Calculus
  - Vertical Approach Comparing the Two Cases: Counterexample Exists/ Counterexample Does Not Exist
- Four-Dimensional Matrix Approach
- Approaches Using the Calculus
- Approach Via Factors of x, y, z
- "Computational" Approaches

We now give an overview of some of these Approaches.

"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.

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 progammer, 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.

In fact, we consider it important to find ways of "generating" $x^{n'} + y^{n'}$ and $z^{n'}$ from $x^n + y^n$, and z^n, where $n' > n$. For further details, see "The Fundamental Challenge of Vertical Approaches" on page 8.

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

The Fundamental Challenge of Vertical Approaches

The fundamental challenge of "Vertical" approaches is to find ways to relate the ordered pairs $<x^k + y^k, z^k>$ and $<x^{k+j} + y^{k+j}, z^{k+j}>$, where $k \geq 1$ and $j \geq 0$. Euler's generalization of Fermat's Little Theorem (see "Fermat's Little Theorem" in Part (4) of this paper, on the web site www.occampress.com) provides us with a means of doing this for $j = \varphi(m)$, where m is a modulus such that $(x, m) = (y, m) = (z, m) = 1$, because the generalization states that $x^k \equiv x^{k + h\varphi(m)}$ mod m, where $h \geq 0$, and similarly for y^k and z^k. The familiar inner product provides us with another means of relating the ordered pairs, in that $<x^k, y^k, z^k> \bullet <x, y, -z> = x^{k+1} + y^{k+1} - z^{k+1}$ (see "Approaches Using Inner Products" on page 24). "Lemma 1.5." on page 13 states several facts that relate the ordered pairs.

Vertical Approach Comparing the Two Cases: Counterexample Exists/ Counterexample Does Not Exist

This Approach relies on the fact that there are terms $u^k + v^k - w^k$, where u, v, w, k are positive integers, that are the same regardless whether a counterexample exists or not. For example, we cannot seriously imagine a professional mathematician saying, prior to Wiles' proof, things like, "Well, of course we know that $17^5 + 6^5 \neq 19^5$, but if a counterexample is proved to exist, then this might change — the value of the difference $19^5 - (17^5 + 6^5)$ might change." We can call this set of terms, 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.

The shortest example of implementation (1) in this paper is "Appendix B: A Possible Simple Proof of FLT", in Part (4) of this paper on the web site www.occampress.com. A lengthier example is described in the next sub-section.

Four-Dimensional Matrix Approach

Consider a four-dimensional matrix M such that cell (u, v, w, k) is occupied by the value of $u^k + v^k - w^k$, where u, v, w, k are positive integers. The matrix makes it possible to speak of the values of neighboring cells, given the value and location of a particular cell: if we know u, v, w, k, then we can compute the value of $u^k + v^k - w^k$, and we can also compute the value of, for example, $(u - 1)^k + v^k - w^k$, which is the value of one of the cells next to that containing $u^k + v^k - w^k$. In fact, there are 8 cells next to each cell except where one of the arguments = 1, because each of the arguments (or "coordinates") can be increased by 1 or decreased by 1. (Obviously, we can generalize this matrix concept to contain the values of any number-theoretic function having m integer arguments, where $m \geq 1$.)

The matrix provides a framework for mathematical induction on any coordinate or any sequence of coordinates — what we might call "crooked induction". We assume that a cell contains 0, which would be the case if a counterexample existed, and then compute the value of each neighboring cell such that at least one of the coordinates is decreased by 1. We then repeat this process until we arrive at a cell the value of whose content is known from other results. If the values differ, then we know that the assumption of a counterexample was false, and thus FLT is proved.

One strategy that uses "crooked induction" is based on the fact that there are cells whose values would not change regardless whether FLT were true or false. For example, we cannot seriously imagine a professional mathematician saying, prior to Wiles' proof, things like, "Well, of course we know that $17^5 + 6^5 \neq 19^5$, but if counterexamples are proved to exist, then this might change — the value of the difference $19^5 – (17^5 + 6^5)$ might change." Certainly the values in the cells immediately surrounding the cell containing a counterexample would differ from the values they would contain if the cell did not contain a counterexample. Can we derive a proof of FLT from these observations?

Further details on the Matrix Approach can be found in part (E) of the section, "Approach Type IV: Considering All Multiples of All Powers of *a, b, c*" in Part (4) of this paper, on the web site occampress.com.

The matrix *M* is the second "geometric" representation of a number-theoretic relation we will introduce in this paper, the first being the lines-and-circles model of congruence (see under "Approaches via the 'Lines-and-Circles' Model of Congruence" in Part (4) of this paper, on the web site www.occampress.com).

"Computational" Approaches

The "Computational" Approaches in the list above were likewise inspired by our work as a programmer, though here the underlying idea is different. In the first computational 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.

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, it would yield the same results if x^p, y^p and z^p were replaced by any positive integers *a*, *b*, *c*, or if *p* were replaced by any positive real in the appropriate range. Perhaps the simplest example of the first of these approaches is that of trying to derive a contradiction by multiplying $(x + y – z)$ and $(x^{p–1} + y^{p–1} + z^{p–1})$ and then deleting x^p, y^p and $–z^p$ from the resulting terms (see "Approaches of Multiplying Integer Polynomials" on page 31). We find, on examining the result, 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 $x^p + y^p \equiv z^p \bmod m$ for all *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 all *m* such that $(a, m) = (b, m) = (c, m) = 1$, 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 46.

So we will try to make it a rule to ask the following question of any approach or strategy: "Does this approach or strategy apply to all *a*, *b*, *c* such that $a + b = $ c?, or to $x^k + y^k – z^k$ where *k* is any positive real in the appropriate range?" If so, then we may be wasting our time. Of course, if we can bring previously-established facts regarding counterexamples into our reasoning, then we may not be wasting our time.

The Lure of the Pythagorean Theorem

In our experience, the most common strategy employed by amateurs is that of attempting to convert an assumed counterexample $x^n + y^n = z^n$ into a Pythagorean equation. This is usually done by writing $(x^{n/2})^2 + (y^{n/2})^2 = (z^{n/2})^2$. We can immediately see one problem with this strategy, namely, that even though this equation must hold if the counterexample equation holds, there is no guarantee that even one of $x^{n/2}$, $y^{n/2}$, $z^{n/2}$ is an integer, and thus there is no guarantee that what is known about Pythogorean triples (integers u, v, w such that $u^2 + v^2 = w^2$) can be applied. One can, of course, apply trigonometric reasoning to the equation.

We believe that, because this strategy was almost certainly worked over in vain during the 300+ years that a proof of FLT was sought, it is unlikely to yield any results in the future.

Most Promising Implementations of Approaches to a Proof of FLT, in Our Opinion

As the reader will discover, this paper contains numerous implementations of the above-described approaches to a proof of FLT. Most of them are attempts at a proof by contradiction. Many of these do not lead to a contradiction (see "The Danger of "Null" Approaches" on page 9), and the others lead to uncertain conclusions because we lack sufficient information about some of the integers involved, "we" here referring to the author, not necessarily to the mathemaical community.

The two approaches that, in our opinion, are most promising, are based on a *comparison* of the two cases (1) a counterexample to FLT exists and (2) a counterexample to FLT does not exist. Such a comparison is not made in the attempts at a proof by contradiction, since only the assumption that a counterexample exists is considered. Of further interest, we believe, is the fact that our proof of the $3x + 1$ Conjecture[1] is likewise based on a *comparison* of the the two cases.

An implementation of the first, and, in our opinion, most promising, approach will be found in "Appendix B: Approach Via the Fixed Set", in Part (4) of this paper, on the web site occampress.com. (A simpler version is given in "A Challenge for Undergraduate Math Majors" on occampress.com.) A description of the second promising approach has already been given under "Four-Dimensional Matrix Approach" on page 8. Referenced sections provide further details.

If our FLT and $3x + 1$ proofs are deemed valid, we believe it will be worthwhile for the mathematics community to try to determine why it is that proofs by contradiction do not seem to work in these cases. Are there facts that lie "outside the reach" of proofs by contradiction, and, if so, why? Do these facts have characteristics that are relatively easy to recognize?

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.

"Appendix B: Approach Via the Fixed Set", in Part (4) of this paper, on the web site occam-

[1] See "A Solution to the 3x + 1 Problem" on occampress.com.

press.com. A simpler version is given in "A Challenge for Undergraduate Math Majors" on occampress.com.

"Four-Dimensional Matrix Approach" on page 8;

;"Approach by a Certain Class of Algorithm" on page 51;

"Third Approach of Multiplying Integer Polynomials" on page 33;

"Implementation" on page 29 (namely, the implementation of our so-far-best approach via the lines-and-circles model of congruence);

"An Approach Via Congruence of Exponents", p. 11 of Part (4) of this paper, on the web site occampress.com

"Second Implementation", p. 18 of Part (4) of this paper, on the web site occampress.com (namely, the second implementation of Approach Type III: Finding a Non-Congruence in a Congruent C-set);

"Appendix B — A Very Simple Approach" on page 55;

"First Implementation of Approach" on page 36 (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 the web site www.occampress.com.

We will offer shared authorship to the first person who makes 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) $(x, y) = (y, z) = (x, z) = 1$.

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

(1.85) Without loss of generality, it suffices to prove FLT 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.)

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" on page 5 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 x. 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 15 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 $x + y > z$.

(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.)

Proof: see "Lemma 0.0: Statement and Proof" on page 8 of Part (2) of this paper, on the web site occampress.com.

Remark:

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

Lemma 0.2

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

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

(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

[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.

at least 3,750,000.

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

Proof: see "Lemma 0.2: Statement and Proof" on page 8 of Part (2) of this paper, on the web site occampress.com.

Lemma 0.3

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

Proof: see "Lemma 0.3: Lemma and Proof" on page 9 of 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" on page 10 of 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" on page 10 of 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" on page 10 of 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, $1 \leq k < p$, *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) $(x^k + y^k)/z^k > (x^{k+1} + y^{k+1})/z^{k+1}$.

[1] Part (a) shows that no Pythagorean triple, i.e., no x, y, z such that $x^2 + y^2 = z^2$, can be elements of a counterexample.

(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 $1 \leq k < p - 1$, *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*, $1 \leq k \leq p - 2$.

(g) $x^k + y^k - z^k \geq Kdef + k - 1$, where here *k* is integral and *Kdef* is as defined in "Lemma 0.2" on page 12. Hence, in particular, since the maximum of the function $x^k + y^k - z^k$ occurs at $p - 1 \leq k < p$, it has value $\geq Kdef + p - 2$.

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

Proof: see "Lemma 1.5: Statement and Proof" on page 11 of 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" on page 14 of Part (2) of this paper, on the web site occampress.com.

Lemma 1.97[1]

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*

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

Proof: see "Lemma 1.97: Statement and Proof" on page 15 of Part (2) of this paper, on the web site occampress.com.

Lemma 2.0

$z < 2y$.

Proof: see "Lemma 2.0. Statement and Proof" on page 16 of Part (2) of this paper, on the web site occampress.com.

Lemma 2.5

$z < x^2$.

[1] 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: Proved by Perisastri in 1969. — Ribenboim, op. cit., p. 236.

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" on page 16 of 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" on page 17 of 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 15 there is a prime p_j between $p_i^{e_i}$ and $p_2^{e_2}$. The result follows by induction. □

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 6 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 under "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 tecnnique. 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.

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).

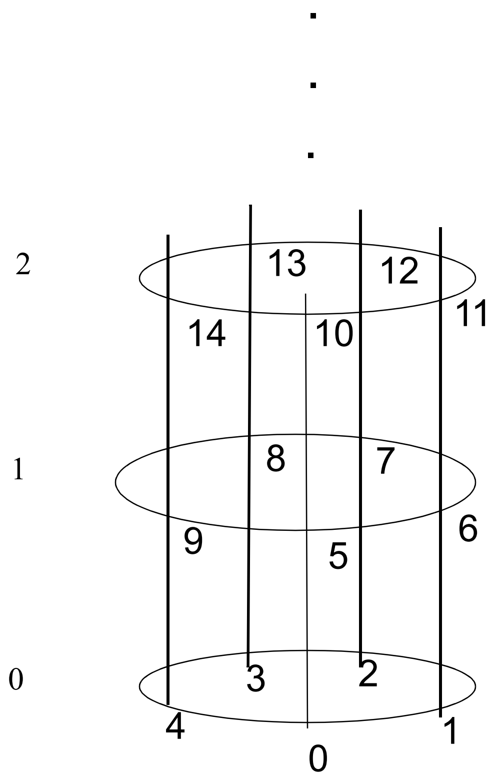

Fig. 1. "Geometrical" model of positive integers congruent mod 5.

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, $14 \div 5$ 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 containing "Type VI" 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.

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 6:

"[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 63.

for all k, $1 \leq k < n + 1$:
$x^k + y^k > z^k$ (part (a) of "Lemma 1.5." on page 13);
$(x^k + y^k)/z^k > (x^{k+1} + y^{k+1})/z^{k+1}$ (part (e) of "Lemma 1.5." on page 13).

for all $k > p = n + 1$:
$x^k + y^k < z^k$ ("Lemma 1.95." on page 14);
$lim\ k \to \infty$, $(x^k + y^k)/z^k = 0$ ("Lemma 1.97" on page 14).

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. In Part 2 of this paper we consider the possible application of the familiar inner product from vector theory to a proof of FLT.

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 13 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 13 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

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

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

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

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

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 13, $p < x < y$, 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 $x =$

[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*."

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 13 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 13), the value of the function at $k = p - 1$ must be $\geq Kdef + p - 1$("Lemma 0.2" on page 12).

(3)

$x^k(\ln x) + y^k(\ln y) - z^k(\ln z) < 0$, $c < k \le p$, 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.,

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

(Although the *slope* of the function $x^k + y^k - z^k$ is negative over this range of *k*, the *value* is positive until $k = p$.)

(5)
ln *u*/ln *v* > *u*/*v*, *u*, *v*, > *e*. (See proof of "Lemma 1.5." on page 13.)

(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?

Approaches Using Inner Products

We can express $x^p + y^p \neq z^p$ as $x^p + y^p - z^p \neq 0$, and we can express a counterexample as $x^p + y^p - z^p = 0$.

The non-counterexample case can also be expressed as $<x, y, z> \bullet <x^{(n-1)}, y^{(n-1)}, -z^{(n-1)}> = x^n + y^n - z^n \neq 0$, where "•" denotes inner product and $n > 2$ but $n \neq p$. The counterexample case can be expressed as $<x, y, z> \bullet <x^{(p-1)}, y^{(p-1)}, -z^{(p-1)}> = x^p + y^p - z^p = 0$.

Definitions

Call an ordered triple <*u*, *v*, *w*>, *u*, *v*, *w* integers, an *inner product term*. (An inner product term is thus a vector.)

For an inner product term <*u*, *v*, *w*>, call <*u*, *v*, *w*> • <1, 1, 1> the *value* of the term. That is, the value of <u, v, w> is simply $u + v + w$.

If we could show that, for u, v, w having the properties of counterexample elements x, y, $-z$, respectively, and for u', v', w' having the properties of x^{p-1}, y^{p-1}, z^{p-1}, respectively, it is not possible that <u, v, w> • <u', v', w'> = 0, then we would have a proof of FLT.

First Approach Using Inner Products

1. Assume that $p = n + 1$ is the smallest exponent such that there exists x, y, z such that $x^{n+1} + y^{n+1} = z^{n+1}$.

2.By part (a) of “Lemma 1.5.” on page 13, we know that *for all k*, $1 \le k \le n$, $x^k + y^k - z^k > 0$, i.e., the value of <x^k, y^k, $-z^k$> is > 0.

By “Lemma 1.95.” on page 14, we know that *for all* $k' > n + 1$, $x^{k'} + y^{k'} - z^{k'} < 0$, i.e., the value of <$x^{k'}$, $y^{k'}$, $-z^{k'}$> is < 0.

3. Let n' be an exponent greater than $n + 1$. Then there are numerous inner products that yield the value of <$x^{n'}$, $y^{n'}$, $-z^{n'}$> = $x^{n'} + y^{n'} - z^{n'}$, which by “Lemma 1.95.” on page 14 we know is less than 0.

For example, consider the product <x^m, y^m, $-z^m$> • <$x^{m'}$, $y^{m'}$, $z^{m'}$>, where $m + m' = n'$, and both m, m' are less than $n + 1$.

But, as we know from part (e) of “Lemma 1.5.” on page 13 (see initial paragraphs under ““Arithmetical” Version of the Approach by Induction on Inequalities” on page 19), each FLT inequality is different from the next at least in the ratio $(x^k + y^k)/ z^k$. Therefore it is reasonable to suspect that the inner products corresponding to differing m, m' such that $m + m' = n'$, will not always yield the same value, much less a value that is less than 0, as required by “Lemma 1.95.” on page 14. If this is the case, we have a contradiction, and a proof of FLT.

Second Approach Using Inner Products

First, some background considerations: We assume that the inner product literature contains an abundance of results concerning which inner products yield 0 and which do not. We would have a proof of FLT if one or more of these results enabled us to establish that:

<x, y, z> • <x^{p-1}, y^{p-1}, $-z^{p-1}$> > 0, where p is the exponent in a counterexample.

In the case of inner products, unlike the case of standard multiplication of the reals, zero divisors exist. Thus, e.g., <2, 1, 0> • <–1, 2, 0> = –2 + 2 + 0 = 0, even though the value of <2, 1, 0> and the value of <–1, 2, 0> are both non-zero.

More generally, let Z denote the set of integers, and let Z × Z × Z denote the Cartesian product. Then Z × Z × Z is a ring, with addition defined by <u_1, v_1, w_1> + <u_2, v_2, w_2> = <$u_1 + u_2$, $v_1 + v_2$, $w_1 + w_2$> and multiplication defined by <u_1, v_1, w_1> • <u_2, v_2, w_2> = <$u_1\, u_2$, $v_1\, v_2$, $w_1\, w_2$> . See, e.g., Durbin, John R., *Modern Algebra: An Introduction*, 4th Ed., John Wiley & Sons, Inc., N.Y., 2000, pp. 116-117.

Now onto our approach: By part (a) of "Lemma 1.5." on page 13 we know that $x + y > z$, or, $x + y - z > 0$ or the value of $<x, y, - z> > 0$. The right-hand side of each of the following equations is positive by "Lemma 1.5." on page 13.

The inner product $<x, y, z> \bullet <x, y, - z> = x^2 + y^2 - z^2$;
The inner product $<x^2, y^2, - z^2 > \bullet <x, y, z> = x^3 + y^3 - z^3$;
The inner product $<x^3 , y^3, - z^3> \bullet <x, y, z> = x^4 + y^4 - z^4$;
...
The inner product $<x^{p-2}, y^{p-2}, -z^{p-2}> \bullet <x, y, z> = x^{p-1} + y^{p-1} - z^{p-1}$.

The inner product $<x^{p-1}, y^{p-1}, -z^{p-1}> \bullet <x, y, z> = x^p + y^p - z^p$ is zero by our assumption of a counterexample.

We recall from linear algebra that

$$\cos\theta = \frac{\langle u, v, w\rangle \bullet \langle r, s, t\rangle}{\|\langle u, v, w\rangle\| \times \|\langle r, s, t\rangle\|}$$

where || <a, b, c> || denotes the length of the vector <a, b, c>, and where θ is the angle between the vectors $<u, v, w>$ and $<r, s, t>$.

In 3-dimensional Cartesian coordinates, let the region containing points $<a, b, c>$ where a, b, and c are each ≥ 0, be called the *positive block*. Let the the region containing points $<a, b, c>$ where a and b are ≥ 0 but $c < 0$ be called the *negative block*. Then the above vectors can be said to point "upward" in the positive block or "downward" in the negative block, and it is easy to see how the existence of a counterexample gives rise to the above pairs of vectors, each pair separated by an angle of 90°.

If we can show that the cosine of the angle between a pair of successive vectors $<x^k, y^k, z^k>$ and $<x^{k+1}, y^{k+1}, z^{k+1}>$, where $2 \le k + 1 \le p$, is > 1, thus contradicting the allowed range of the cosine function for the value of the angle between different vectors, then we would have a proof of FLT

A closely related approach is the following: $<x, y, z>$ and $<x^{p-1}, y^{p-1}, -z^{p-1}>$ are vectors in 3-dimensional Cartesian space. Each lies on a line from the origin <0, 0, 0>. If x, y, z, p are in fact constituents of a counterexample, then the vectors must be perpendicular, since this is the only way that their inner product can be 0 (that is, the only way that the angle between them can be 90°). Fig. 2 shows the points and the lines defined by the vectors:

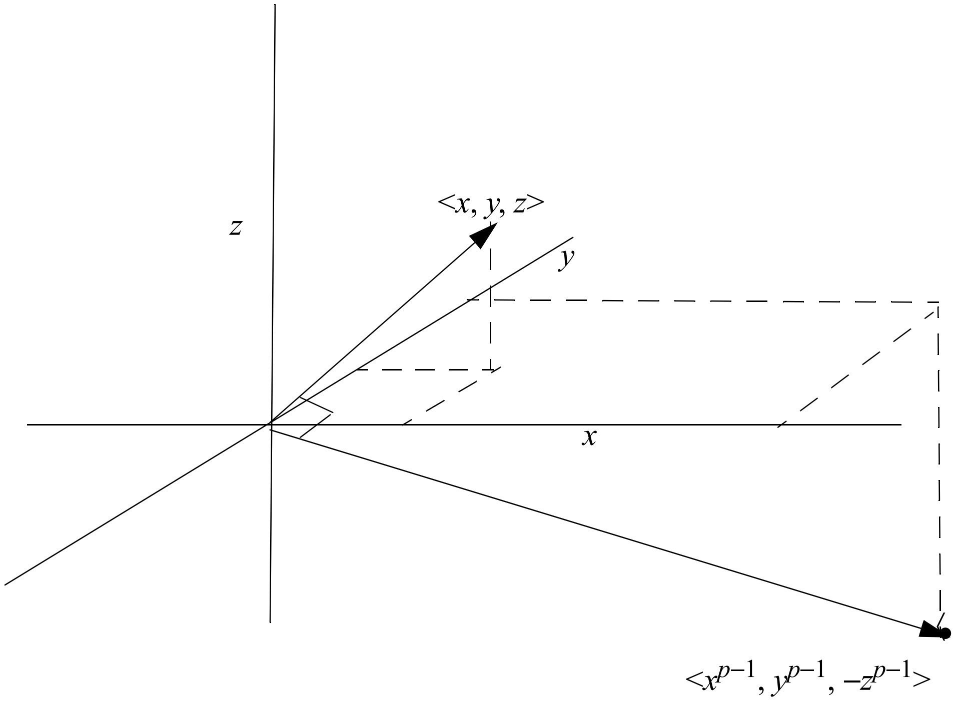

Fig. 2 The vectors, hence lines from the origin, defined by the points <x, y, z> and <x^{p-1}, y^{p-1}, $-z^{p-1}$>.

If we write the equations for the two lines and find that the point <x^{p-1}, y^{p-1}, $-z^{p-1}$> is not on the lower line, then we have a proof of FLT.

Fourth Approach Using Inner Products

(The Third Approach has been deleted.)

We next ask: Is it really possible that a succession of inner products — around 125,000 as of 1990, since as of that date, FLT had been proved for all primes up to around 125,000, and in our succession of products here, we use all exponents, not merely primes — each of whose terms is positive, and the value of each of which is positive, could suddenly yield an inner product whose value is zero? We know, of course, as a result of Wiles' proof, that the answer is no, so our question should be phrased: Is it really possible that we can not prove, using existing results on inner products as of the early nineties, that a succession of inner products, each of whose terms is positive, and the value of each of which is positive, can not suddenly yield an inner product whose value is zero? The following is an attempt to prove that an inner product whose value is zero is not possible

$a = x^{p-1}$;
$b = y^{p-1}$;
$c = z^{p-1}$;
$d = x$;

$e = y$;
$f = z$.
We now begin an attempt to show that $<a, b, c> \bullet <d, e, -f> = ad + be - cf \neq 0$, the truth of which would give us a proof of FLT.

Since $d + e - f > 0$ (by part (a) of "Lemma 1.5." on page 13), we can multiply through by $a, b,$ and c and get:
$ad + ae - af > 0$;
$bd + be - bf > 0$;
$cd + ce - cf > 0$,

Similarly, since $a + b - c > 0$ (by part (a) of "Lemma 1.5." on page 13), we can multiply through by d, e, f and get:

$da + db - dc > 0$;
$ea + eb - ec > 0$;
$fa + fb - fc > 0$.

Are these inequalities, plus the constraints on x, y, z given earlier in this paper, sufficient to show that $ad + be - cf \neq 0$, and hence to prove FLT?

A relalated approach is the following:

By Lemma 0.0, we know that $x + y - z > 0$. Certainly $x^{p-1} + y^{p-1} + z^{p-1} > 0$. Therefore $(x + y - z) \times (x^{p-1} + y^{p-1} + z^{p-1}) > 0$. Multiplying out, we get:

(1)
$x^p + xy^{p-1} + xz^{p-1} +$
$yx^{p-1} + y^p + yz^{p-1} +$
$-zx^{p-1} - zy^{p-1} - z^p$.

By assumption, $x^p + y^p - z^p = 0$ so we can eliminate these terms from (1). Collecting the remaining terms we get: $x^{p-1}(-z + y) + y^{p-1}(-z + x) + (x + y)z^{p-1}$. Now since, by "Lemma 1.0." on page 13, $x < y < z$, it follows that $x^{p-1}(-z + y) + y^{p-1}(-z + x)$ is negative. It was known[1], prior to the 1990s, that it was possible that $z - y = 1$, so it is possible that $-z + y = -1$. By Lemma 1.0, $-z + x > -y$. Are these facts, in addition to the fact, established by part (a) of "Lemma 1.5." on page 13, that $x^{p-1} + y^{p-1} > z^{p-1}$, sufficient to enable us to prove that (1) is negative, thus giving us a contradiction? It seems not.

Fifth Approach Using Inner Products

1. As we stated in the "Second Approach Using Inner Products" on page 25, the ordered triples $<x, y, -z>$, and $<x^k, y^k, z^k>$ where $1 \leq k \leq p - 1$ can each be regarded as a vector in 3-dimen-

[1] Ribenboim, Paolo, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, N.Y., 1979, p. 64.

sional space.

2. Assume a counterexample exists. Then the inner product $<x, y, -z> \bullet <x^{p-1}, y^{p-1}, z^{p-1}> = x^p + y^p - z^p = 0$. By a basic fact of linear algebra, this implies that the angle between the two vectors is 90 degrees.

3. It follows that, for each j, $1 \leq j \leq p - 1$, there is a pair of vectors $<x^j, y^j, -z^j>$, $<x^{p-j}, y^{p-j}, z^{p-j}>$ that are at an angle of 90 degrees to each other.

At present, we do not see any way to make a proof of FLT out of this simple fact. We point out in passing that, since each pair of vectors forms a right angle, the vectors are the legs of a right triangle whose hypotenuse is $<x^j + x^{p-j}, y^j + y^{p-j}, -z^j + z^{p-j}>$. By the Pythagorean Theorem, we then have

$$((x^j)^2 + (y^j)^2 + (z^j)^2) + ((x^{p-j})^2 + (y^{p-j})^2 + (z^{p-j})^2) =$$

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

Multipliying out the right-hand side, we see that the equation is true only if $2x^p + 2y^p - 2z^p = 0$, which, by assumption of a counterexample, is true.

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:

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

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.

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 9.

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 12) and integral, the product must be a positive integer $>$ $(x^{p-1} + y^{p-1} + z^{p-1})$.

.Multiplying out the product, we get:

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

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

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

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

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

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 13. Thus $0 < h < x^p$. By part (g) of "Lemma 1.5." on page 13, 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 13, 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)

[1] Simply set $x + y = z + Kdef$ (by part (a) *of* "Lemma 1.5." on page 13), yielding $x = z - y + Kdef$. Then multiply through by y, and set $zy = z + z(y - 1)$.

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

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

By part (a) of "Lemma 1.5." on page 13, 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.

We point out that on the right-hand side of (1), x^{p-1}, y^{p-1}, and z^{p-1} are each multiplied by a term that is less than the corresponding term, namely, $(x + y + z)$, on the left-hand side. Since $(x^{p-1} + y^{p-1} - z^{p-1})$ is a positive term (by part (g) of "Lemma 1.5." on page 13), does this provide us with a contradiction that would yield a proof of FLT?

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 13, we know that

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

2. Now for all positive integers u and 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 13, $x < y < z$. 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 13 $x + y > z$, 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)

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

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

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 13, 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)
$S = (x^1 + y^1 - z^1) + (x^2 + y^2 - z^2) + (x^3 + y^3 - z^3) + ... + (x^{p-1} + y^{p-1} - z^{p-1})$.

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

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

We ask if the assumption of a counterexample results in a value of (2) that is clearly less than (1). We observe in passing that, since, by part (b) of “Lemma 1.5.” on page 13, $(x^k + y^k - z^k) < x^k$., we have
\

$$S < \left(\frac{x^p - 1}{x - 1} - 1\right)$$

If the value of the expression

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

in (2) is positive, then we have a contradiction, and a proof of FLT, because it is not possible that $a + b < a$, where a, b are positive.

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 writing the right-hand side of (2) in the previous sub-section as

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

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 13, $p < x < y < z$, 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

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

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

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

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

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

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 13;
property (d) corresponds to part (e) of "Lemma 1.5." on page 13.

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 importance for our approaach. We draw the reader's attention to the fact that, by part (g) of "Lemma 1.5." on page 13, $x^k + y^k - z^k \geq (Kdef + k - 1)$, 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:

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

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

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

.

.

.

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

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

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

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

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

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

$$\vdots$$

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

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

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, $1 \leq k \leq p$. 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, $3 \leq k \leq p$.

We now prove two very elementary lemmas. Let:

(6) $\mathrm{B}_{n, (z - y)} = (z^{n-1} + z^{n-2}y + \ldots + zy^{n-2} + y^{n-1})$.
$\mathrm{B}_{n, (z - x)} = (z^{n-1} + z^{n-2}x + \ldots + zx^{n-2} + x^{n-1})$.
$\mathrm{B}_{n, (x + y)} = (x^{n-1} - x^{n-2}y + \ldots + y^{n-1})$, $n \geq 3$.

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 very elementary lemma.

Lemma 28.0.

$((z - y), (z - x), (x + y)) = 1$, i.e.*, the three terms do not have a factor in common.*

Proof of Lemma 28.0:
The proof is by contradiction.

1. Assume that the three terms do have a factor q in common, and without loss of generality, assume q is a prime. Then:

(20) $z - y \equiv 0 \bmod q$,
(21) $z - x \equiv 0 \bmod q$,
(22) $x + y \equiv 0 \bmod q$.

2. Adding (20) and (22) yields
(23) $x + z \equiv 0 \bmod q$,

which with (21) yields

(24) $2z \equiv 0 \bmod q$

implying $z \equiv 0 \bmod q$. This with (21) implies $x \equiv 0 \bmod q$, contradicting (1.5). □

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 $B_{p, (z-y)}$;
(E.2) The exponent p divides only $(z - y)$ but not $B_{p, (z - y)}$;

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

(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

$G' = \{ ..., 1/(B_{3, (z - y)}), 1/(B_{2, (z - y)}), 1, (z - y)B_{2, (z - y)}, (z - y)B_{3, (z - y)}, ...\}$

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

[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.

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

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[1] 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?

Approaches Using the Calculus

First Vertical Approach Using the Calculus

1. The continuous function $f(k) = x^k + y^k - z^k$, $1 \leq k \leq p$ has the properties that $f(k)$ increases monotonically from an initial positive number to a maximum at $f(p{-}1)$, then decreases monotonically to 0 at $k = p$ ("Lemma 1.5." on page 13). (See figure in the sub-section, "Second Vertical Approach Using the Calculus" on page 47.) The maximum is greater than or equal to $Kdef + p - 2$, where $K = 2pU$, $U \geq 1$, each of d, e, f is greater than 1 ("Lemma 1.5." on page 13), and $p \geq 125{,}000$, by results established prior to Wiles' proof of FLT in the early nineties.

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

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

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

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

[1] 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.

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

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

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

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 13, $x^{p-1} + y^{p-1} - z^{p-1}$ 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 13); 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. Therefore, by “Lemma 1.5.” on page 13, 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

Note added later: We have here failed to recognize a “Null” Approach, as decribed under “The Danger of “Null” Approaches” on page 9. Specifically, we have failed to realize that the large positive number and the large negative number are not limited to the case of the prime exponent p in our assumed counterexample. For, it is easily shown that there must be a $k > (p - 1)$ such that $x^k + y^k - z^k = 0$. Of course, there is no requirement that k be an integer.

In passing, we make the following observations:
There exist k', k'', k''' each between 0 and 1 such that;
$x^{k''} = (x-1)$;
$y^{k'''} = (y-1)$;
$z^{k'} = (z-1)$;
It is clear that, since $x < y < z$, $k'' < k''' < k'$.
Then
$x^{p-1}x^{k''} + y^{p-1}y^{k''} - z^{p-1}z^{k''} > 0$, by Lemma 1.5; hence
$x^{p-1}x^{k''} + y^{p-1}y^{k'''} - z^{p-1}z^{k''} > x^{p-1}x^{k''} + y^{p-1}y^{k''} - z^{p-1}z^{k''}$ (the y term is greater);
$x^{p-1}x^{k'} + y^{p-1}y^{k'} - z^{p-1}z^{k'}$ > either of the previous two expressions, by Lemma 1.5, hence > 0.

Second Vertical Approach Using the Calculus

Let $f(k)$ denote the function $x^k + y^k - z^k$, where x, y, z are constituents of an assumed minimal counterexample, and k is real and ≥ 1. Clearly, f is continuous and has a derivative for all k.

The maximum value of f over the range $1 \leq k \leq p$ is $\geq Kdef + (p-1) - 1$ and occurs in the interval $p - 1 \leq k \leq p$ (part (g) of “Lemma 1.5.” on page 13).

Consider the right triangle ABC (see Fig. 3), where A is the point $(p-1, 0)$, B is the point

$(p-1, x^{p-1}+y^{p-1}-z^{p-1})$ and C is the point $(p, 0)$. Let θ denote the angle ACB. Then $tan\ \theta = -(x^{p-1}+y^{p-1}-z^{p-1})/(p-(p-1)) = -(x^{p-1}+y^{p-1}-z^{p-1})$.

Note added later: in the sub-section, "On the Maximum of the Function f(k)" on page 49, we show that the maximum of the function $f(k)$ must occur at $k > p-1$. So the strategy in this sub-section will probably not be successful.

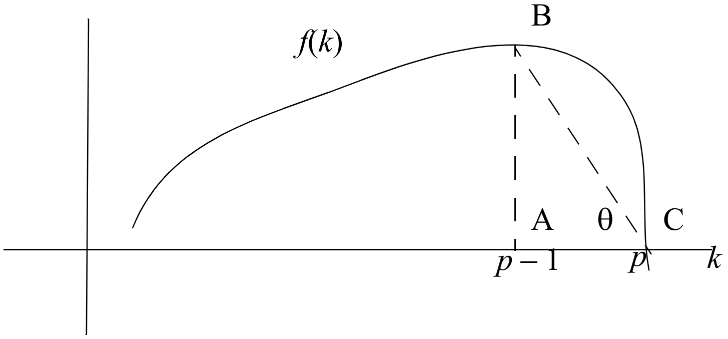

Fig. 3 Graph of the function *f*(*k*)

By the mean-value theorem for derivatives, there exists a point k in the interval $p-1 \leq k \leq p$ such that the derivative, $f'(k)$, of $f(k)$ with respect to $k = tan\ \theta$. By an elementary fact of the calculus, $f'(k) = x^k(ln\ x) + y^k(ln\ y) - z^k(ln\ z)$. We ask if $tan\ \theta$, which equals $-(x^{p-1}+y^{p-1}-z^{p-1})$ because θ is a negative angle, equals $x^k(ln\ x) + y^k(ln\ y) - z^k(ln\ z)$ for the point k required by the mean-value theorem. If we can prove that the answer is no, then we have a proof of FLT.

Although $-(x^{p-1}+y^{p-1}-z^{p-1})$ is a negative integer, it is at first hard to believe that $f'(k) =.x^k(ln\ x) + y^k(ln\ y) - z^k(ln\ z)$ is also a negative integer, given the nature of the natural logarithm of integers. However, whether it is hard to believe or not, we must keep in mind that at some point $k \geq p-1, f'(k) = 0$. Furthermore, we know from part (g) of "Lemma 1.5." on page 13 that $|-(x^{p-1}+y^{p-1}-z^{p-1})| > 3p$, and p, prior to Wiles' proof, was known to be greater than 125,000. So, since $f'(k) = x^k(ln\ x) + y^k(ln\ y) - z^k(ln\ z)$ is continuous, its values pass through the integer values 1, 2, 3, ..., 125,000, ... Thus it is entirely possible for $f'(k)$ to have an integer value at the k required by the mean-value theorem.

If we can prove that $x^k(ln\ x) + y^k(ln\ y) - z^k(ln\ z)$ is irrational, then we will have a contradiction, and hence a proof of FLT, because this will imply that the function $f(k)$ cannot cross the k axis at the integer p. Unfortunately, even if $(ln\ x)$, $(ln\ y)$, and $(ln\ z)$ are each irrational (a plausibility argument is given in the next paragraph), this does not prove that the *sum* $x^k(ln\ x) + y^k(ln\ y) - z^k(ln\ z)$ is irrational. In passing, we observe that if the sum of any *two* terms in the three-term sum is rational, then the entire sum is irrational, because the sum of a rational and an irrational is irrational.

Our plausibility argument is as follows: Assume, to the contrary, that the natural logarithm of the positive integer c is the rational a/b, i.e., assume that $e^{a/b} = c$, where a, b, c are positive integers, and a/b is in lowest terms and is greater than, say, 10. Raise both sides of the equation to the bth power, and get $e^a = c^b$. For the left-hand side we have $(e)(e)(e) \ldots (e)$ (a terms). The only way that this product can yield the integer c^b is if all digits to the right of the decimal point are 0s, or if all digits to the right of the decimal point are 9s. But since e is irrational, we argue that the first case is not possible. Since $u.0000... = (u-1).9999...$, where u is a positive integer, we argue that the second case is therefore also not possible. Of course, we have not even considered the possibile irrationality of x^k, y^k, and z^k.

The following may be worth some investigation. We know that there exists a $k \geq p - 1$ such that $f\,'(k) = x^k(ln\ x) + y^k(ln\ y) - z^k(ln\ z) = 0$. By assumption of a counterexample, we know that $x^p + y^p - z^p = 0$. Subtracting the first equation from the first implies $x^k(x^{p-k} - ln\ x) + y^k(y^{p-k} - ln\ y) - z^k(z^{p-k} - ln\ z) = 0$. Now, $u^{p-k} - ln\ u < u^{p-k}$, where $u = x\ or\ y\ or\ z$, and so it is natural to wonder if we have a contradiction to the fact that there is no exponent $r < p$ such that $x^r + y^r - z^r = 0$.

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

In the previous sub-section, we showed that 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, reaches a maximum at $k \geq (p - 1)$ ("Lemma 1.5." on page 13), then descends monotonically to 0 at $k = p$ (see "Lemma 1.5." on page 13), 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 $p - 1 < k < p$.

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

(a′), (b′), (c′) imply

(a″) x and $(z - y)$ have a factor geater than 1 in common, i.e., $(x, z - y) = d$, where $d > 1$;
(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 11, $(x, y) = (y, z) = (x, z) = 1$, 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?

"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.

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 Algorithm

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 consists 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
> ...

Define an algorithm $prog(x, y, z, n)$, where x, y, z, n are positive integers such that if $x^n + y^n \neq z^n$ then $prog(x, y, z, n) = 0$, *and* if $x^n + y^n = z^n$ then $prog(x, y, z, n) = 1$.

Now define a second algorithm $prog'(x, y, z, n)$, where x, y, z, n are all positive integers, such that $prog'(x, y, z, n) = 0$ for all x, y, z, n.

We have now reduced the question of the truth of FLT to a question of whether two algorithms compute the same function.

It is clear that $prog'$ is a member of the Class defined at the start of this sub-section. Let us assume we can prove that $prog$ is also a member of the Class, and that $prog$ consists of u instructions. Then if $prog$ returns 0 for all inputs of length $x + 1$ (and almost certainly this was true for all inputs for which FLT was known to be true before 1990), then $prog$ computes the same function as $prog'$ by the argument given in our paper cited above. And thus FLT is proved.

Approach by "The Extra +"

Description

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 procedure, call it F. In other words, the same procedure F can generate all possible instances of the left-hand and right-hand sides, with $0^n = 0$ being always added on the right. Furthermore, 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 procedure called, say, *incr*.) By "in unison" we mean that the execution of *incr* during the course of computing the left-hand side, always takes place in the same time period as the execution of *incr* on the right-hand side.

We can therefore write a program P that operates as follows:

For x, y, z as constituents of a possible counterexample to FLT, P computes the left-hand and the right-hand sides of the FLT inequality for $n = 3$ and compares the results. If they are equal (which we know will not be the case, of course), the program halts. If they are unequal, the program repeats the process for $n = 4$, $n = 5$, etc. We will have a proof of FLT if we can prove that P never halts. Without loss of generality, we can write P so that the procedure that computes u^n, where $u = x$, y, or z, or 0, always does this by multiplying u by $u^{n\text{-}1}$. We do this in the belief that it will increase our chances of discovering why the left-hand side and the right-hand side must always be unequal.

In order to further increase our chances of proving that the left-hand and the right-hand sides are always unequal, P is to be written as a Turing machine.

In passing, we note that P can be thought of as a computational implementation of the "Vertical Approaches by Induction on Inequalities" on page 19.

Now suppose that we install two counters, C_L and C_R, in P. Both are set to 0 when P starts executing. C_L counts the number of successive invocations of *incr* that occur when P computes the left-hand side of the FLT inequality. C_R counts the the number of successive invocations of *incr* that occur when P computes the right-hand side of the FLT inequality .

Proof Strategy

Assume, now, that FLT is false, or, in other words, that for some x, y, z, p as described above under "Initial Assumptions, Definitions, and Properties of Numbers Involved" on page 11, $x^p + y^p = z^p$. Then after P has computed $z^p + 0^p$, the counter C_R will show z^p incrementations. But after P has completed execution of x^p and y^p, the counter C_L will likewise show (by hypothesis) a total of z^p increments. *But P 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 completes computation of $x^p + y^p$. Thus, contrary to hypothesis, and in conformity with fact, $x^p + y^p \neq z^p$.

Discussion

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.

One answer is: the Approach *does not apply to such x, y, z*, because, by Lemmas 0.0 and 0.5, there are no such x, y, z that can be counterexamples to FLT, and the Approach is based on the assumption that x, y, z are elements of such a counterexample!

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. **r** is then

[1] by Monsur Hossain

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 (e.g., the context in which the exponent of $x, y, z = 1$ or 2). 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.

In reply to the argument that the Approach proves that for no x, y, z does $x + y = z$ (which is contrary to fact) we might point out that there are no increments-by-1 to be counted on the right-hand side of the equation. I.e., the Approach does not apply to this case. But then we must explain why the Approach does not prove that, e.g., there are no x, y, z, w, u, v such that $x + y = z + w + u + v$, which is also contrary to fact. Here, of course, there is addition, hence incrementation-by-1 on the right-hand side.

We should also consider a possible application of the "Vertical Approach" (see "Brief Summary of Approaches Described in This Paper" on page 6) 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.

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 — A Very Simple Approach

This Approach has been moved to the sub-section “First Vertical Approach Using the Calculus” on page 46.

Appendix C — Probably the Most Popular Very Simple Approach

The following was motivated by an unpublished paper by, and subsequent discussions with, Richard Van Elburg,

If there is one Approach that has been favored by amateurs over the years (beyond those that attempt to use the Pythagorean Theorem (see "The Lure of the Pythagorean Theorem" on page 10)) it is probably the following: express two of x, y, z in terms of a 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. In any case 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 12, $x + y > z$, equation (3) can only hold if $i + j < k$. We have already established (3) in part (a) of "Lemma 0.2" on page 12.

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 13), we therefore can state, if "(1.91) (c)" on page 6 of 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 13we 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 13, $p < x < y < z$, 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.

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 13).

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 13
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 13
For all k, $1 \le k \le (p - 1)$, $x^k + y^k > z^k$.	Part (a) of "Lemma 1.5." on page 13
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 13
For all $k > p$, $x^k + y^k < z^k$.	"Lemma 1.95." on page 14
$p < x < y < z$.	"Lemma 1.0." on page 13
$p > 125{,}000$ *(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 14
$z < x^2$.	"Lemma 2.5" on page 14
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 15
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 (4) 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" on page 3 of Part (2) of this paper, on the web site occampress.com.
Let p, q, be odd primes, and let t be a positive integer. Then there exists an infinity of primes q such that $(p, q - 1) = (t, q - 1) = 1$.	"Lemma 3.0. Statement and Proof" on page 16
$((z - y), (z - x), (x + y)) = 1$, i.e., *the three terms do not have a factor in common*.	"Lemma 28.0." on page 43
$$\lim_{k \to \infty} \frac{x^k + y^k}{z^k} = 0$$	"Lemma 1.97" on page 14

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 43

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.