Is There a “Simple” Proof of Fermat's Last Theorem? A New Approach

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

June 10, 2005

Key words: Fermat's Last Theorem

Introduction

Fermat's Last Theorem (FLT) states that:

For all $n > 2$, 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 $n > 2$. 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 350 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 used to prove FLT for $n = 4$. This method can actually be used to prove a stronger statement than

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

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:

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

"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 the author's computer screen)

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, 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?

The author is well aware that the overwhelming consensus in the mathematics community is that no simple proof of FLT exists. So the reader is perfectly justified in asking, "Why bother spending even five minutes more on the question of a 'simple' proof?" The author thinks there are several reasons:

- The computer has pushed the deductive horizon far beyond that of even the best mathematicians of the past, where by "deductive horizon" the author means the limit of our ability to carry out long deductions. For example, the author believes 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 page26.

- New conceptual machinery is constantly appearing that might make a simple proof possible. The author is thinking specifically of computation theory. An attempt to use some of this machinery is given in the section ""Computational" Approaches" on page26.

- 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. The author was told by several professional mathematicians prior to Wiles' proof, that whenever an envelope arrives on their desk containing a manuscript with "Fermat's Last Theorem" in the title, and the manuscript is by an author who is not a tenured professor, the manuscript goes 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 know now that it is true. No doubt all, or very nearly all, of the manuscripts that mathematicians received from amateurs[1] 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, contained the germ of an idea that might have led to a "simple" proof ofFLT. 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 a friend.

- 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. The author believes that the approaches described under "Approach by "Geometry of Congruences"" on page10 and under ""Arithmetical" Version of the Approach by Induction on Inequalities" on page17 might be among these.

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
    - Approach by "Geometry of Congruences"
    - Approach by Induction on Inequalities
- "Computational" 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 Frénicle de Bessy, that he had proved the Theorem for the case $n = 4$; but he did not give full details[2]. Euler gave an incomplete proof for the case $n = 3$ in the early 18th century;

[1] And yet Fermat, and Pascal, and many of the leading mathematicians of the 17th century were amateurs!

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" primes, a class of primes he defined. Among the primes < 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. The author will call this 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 the author calls 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, 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. This is, in fact, the form in which the Vertical Approach first occurred to the author when he became interested in FLT. The author was at the time working as a progammer, and thus immediately thought about the task of trying to find a counterexample using the computer.

The "Computational Approaches" in the list above were likewise inspired by the author's work as a programmer, though here the underlying idea is different. The first computational approach is based on the behavior of a program that could compute both the left-hand and right-hand sides of the FLT inequality. The second computational approach is based on an idea from algorithmic information theory.

Most Promising Approaches, in the Author's Opinion

At present, the author believes that the following are the most promising approaches to a "simple" proof of FLT:

"An Attempted Implementation of the Approach by "Geometry of Congruences"" on page15.
"Strategy Using Ratios Between FLT Inequalities" on page18;

The author will pay $150 to the first person who can find errors in both these approaches such that the author cannot repair all the errors in at least one approach, within five days. Furthermore, the author will offer shared authorship to the winner of the prize if he or she can fix the errors in at least one approach in a way that leads directly to publication. *Note: before submitting descriptions of errors, competitors for the prize must query the author as to the current status of the prize. The prize will not be awarded 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:

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

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

1. We will use proof by contradiction. That is, we will assume there exist positive integers x, y, z such that for some $n > 2$,

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

2. Without loss of of generality, we let $n = p$, the smallest odd prime such that (1) holds. Therefore from now on, we will usually write p instead of n when referring to an assumed counterexample.

3. Also 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.

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 of Lemma 0.0.
Assume the contrary, i.e., that $x + y \leq z$. Then, in the case that $x + y = z$, $(x + y)^p = z^p$. By the binomial theorem, this implies that:

$$x^p + \binom{p}{1}x^{p-1}y + \ldots + \binom{p}{p-1}xy^{p-1} + y^p = z^p$$

Clearly, the equation cannot hold if $x^p + y^p = z^p$. A similar argument applies if $x + y < z$. □

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

Lemma 0.5.
If $x^2 + y^2 = z^2$, then x, y, z cannot be elements of a counterexample.

Proof 1 of Lemma 0.5:

Follows directly from Lemma 0.0. □

Proof 2 of Lemma 0.5:

1. Let $x^2 + y^2 = z^2$.

2. Raise both sides of this equation to the power $p/2$. We get:

$$x^p + y^p < (x^2 + y^2)^{p/2} = (z^2)^{p/2} = z^p$$

□

Remark:
Lemma 0.5 states that no elements of a Pythagorean triple can be elements of a counterexample.

Examples of Lemma 0.5:
$3^2 + 4^2 = 5^2$, but $3^3 + 4^3 < 5^3$ (27 + 64 = 91, which is < 125), and $3^{11} + 4^{11} < 5^{11}$ (177,147 + 4,194,304 = 4,371,451, which is < 48,828,125). $7^2 + 24^2 = 25^2$, but $7^3 + 24^3 < 25^3$ (343 + 13,824 = 14,167, which is < 15,625).

Lemma 0.6
If FLT is true for the exponent n, then it is true for all multiples of n.

Proof of Lemma 0.6:
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 $u, v, w, k \geq 1$. □

Lemma 1.0.
$p < x < y < z$.

Proof of Lemma 1.0.
We quote from Ribenboim, Paulo, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, N.Y., 1979, p. 226.

"In 1856, Grünert proved:

"(1A) If $0 < x < y < z$ are integers and $x^n + y^n = z^n$, then $x > n$.

"Proof:

“$x^{n\,=} z^n - y^n = (z - y)(z^{n-1} + z^{n-1}y + \dots + y^{n-1}) > (z - y)ny^{n-1}$.
“Hence

$$0 < (z - y) < \frac{x^n}{ny^{n-1}} < \frac{x}{n}$$

“and

$$y + 1 \leq z < y + \frac{x}{n}$$

“so $n < x$.”

Lemma 2.0.
$z < 2y$.

Proof of Lemma 2.0.
$x^n + y^n < 2y^n < (2y)^n$, so z cannot be $\geq 2y$. □

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 the author asks the question here is that he has not come across it in the FLT literature he has 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.

However, as a mathematician has pointed out to the author, there does not exist a non-trivial factorization of P over any of 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 page5 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 below under "An Attempted Implementation of the Approach by "Geometry of Congruences"" on page15. 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.

Approach by "Geometry of Congruences"

In this Approach, we attempt to show that the assumption of a counterexample implies a contradiction between congruences pertaining to the counterexample, and congruences pertaining to exponents for which FLT is known (say, pre-1990) to be true.

Preliminaries

The "Lines-and-Circles" Model of Congruence

The Approach is 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).

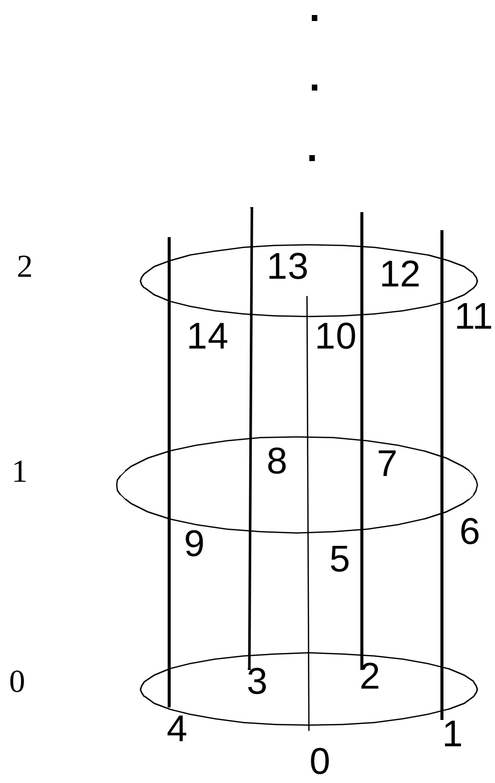

Figure 1. "Geometrical" model of positive integers congruent mod 5.

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

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

In the "Geometry of Congruences" Approach, we define a *potential counterexample* <*x*, *y*, *z*, *n*, *m*> (here *n* need not be a prime) as a congruence $x^n + y^n \equiv z^n$ mod *m*, and we imagine x^n, y^n, and z^n as occupying positions on the vertical lines in our geometrical model of congruence mod *m*. Similarly, we define a *non-counterexample* <*x*, *y*, *z*, *n*, *m*> as a congruence $x^n + y^n$ is not $\equiv z^n$ mod *m*, and we imagine x^n, y^n, and z^n as occupying positions on the vertical lines in our geometrical model of congruence mod *m*. (The justification for our calling the non-congruence a non-counterexample is (1.91) (c) below.) We then consider, for a given modulus *m*, the relationship between potential counterexamples, and the relationship between non-counterexamples.

Congruences Pertaining to Equalities, and Congruences Pertaining to Inequalities

We will be using several facts of elementary number theory that relate congruences pertaining to equalities, and congruences pertaining to inequalities. These facts are as follows:

For equalities:

(1.90)

(a) If $a + b$, $c < m$, and $a + b = c$, then $a + b \equiv c \bmod m$.

(b) If $a + b \equiv c \bmod m$, *and* $a \equiv a' \bmod m$, and $b \equiv b' \bmod m$, and $c \equiv c' \bmod m$, *then* $a' + b' \equiv c' \bmod m$.

For inequalities:

(1.91)

(a) If $a + b$, $c < m$, and $a + b \neq c$, then $a + b$ is not $\equiv c \bmod m$.

(b) Assume $a \equiv a' \bmod m$, and $b \equiv b' \bmod m$, and $c \equiv c' \bmod m$. Then:
If $a + b$ is not $\equiv c \bmod m$ then $a' + b'$ is not $\equiv c' \bmod m$.

Proof of (1.91) (b):
If $a \equiv a' \bmod m$, and $b \equiv b' \bmod m$, and $c \equiv c' \bmod m$, then, by definition of congruence, this implies that there exist integers h, j, k such that $a' = a + hm$, $b' = b + jm$ and $c' = km$.

We prove the contrapositive of our statement.

Assume $a' + b' \equiv c' \bmod m$. Then by definition of congruence, this implies that $a + b + (h + j - k)m = c$, which by definition of congruence implies that $a + b \equiv c \bmod m$. □

(c) If $a + b$ is not $\equiv c \bmod m$, *then* $a + b \neq$ c.

In addition, we will need Fermat's Little Theorem:

(1.92)

If q is a prime and $(a, q) = 1$ then $a^{q - 1} \equiv 1 \bmod q$.

Multiplying both sides of the congruence in (1.92) repeatedly by a yields

$a^{(q - 1) + 1} \equiv a \bmod q$,
$a^{(q - 1) + 2} \equiv a^2 \bmod q$,
$a^{(q - 1) + 3} \equiv a^3 \bmod q$,
...

Thus $(q - 1)$ is a modulus that defines a set of $(q - 1)$ congruence classes.

Discussion of the Approach by "Geometry of Congruences"

Given three positive integers a, b, and c, exactly one of two possibilities must hold: either $a +$

$b = c$ or $a + b \neq c$. However, when we bring congruence into the picture, more possibilities present themselves. First, we can have, for $m \geq 2$:

$a + b \equiv c \bmod m$, in which case $a + b$ may or may not equal c;
$a + b$ is not $\equiv c \bmod m$, in which case, by (1.91) (c) we know that a + b ≠ c.

Second, congruence mod m for any $m \geq 2$, allows us to "reduce the infinite to the finite". That is, it enables us to partition, in a systematic way, the infinite set of positive integers into a finite set of m congruence classes. And, thanks to Fermat's Little Theorem, and Euler's Generalization of the Theorem[1], it allows us, for appropriate m, to "reduce the infinite set of powers of integers to the finite". That is, it allows us to partition the infinite set of powers into a finite set of congruence classes — $q - 1$ classes in cases where Fermat's Little Theorem applies (see (1.92)).

To give an example of how this reduction into finite classes might be of use in our pursuit of a proof of FLT, consider the following lemma.

Lemma 4.0.
Assume a counterexample $x_c^p + y_c^p = z_c^p$ exists. Then p cannot be a member of a certain infinite set of primes.

Proof of Lemma 4.0
1. Assume a counterexample $x_c^p + y_c^p = z_c^p$ exists. By assumption (1) above, p is the smallest such prime.

2. As proved under "Discussion" on page28, it is not possible that $x_c + y_c = z_c$.

3. Let q be *any* prime such that $(x_c, q) = (y_c, q) = (z_c, q) = 1$ and $x_c + y_c$, z_c are $< q$. Such a prime must exist because there are an infinite number of primes and only a finite number of prime factors, total, in x_c, y_c, and z_c .

4. By (1.92), (q - 1) defines a set of (q - 1) residue classes mod (q - 1). For the class whose minimum element is 1, we have, by step 2,

(1.95) $x_c^{1 + k(q-1)} + y_c^{1 + k(q-1)}$ is not $\equiv z_c^{1 + k(q-1)} \bmod q$,

where $k \geq 0$.

[1] The Generalization asserts that if $(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \bmod m$, where $\phi(m)$ is Euler's totient function, which returns the number of numbers less than m and relatively prime to m.

5. Dirichlet's celebrated Theorem states that the infinite series $\{a + v\,b\}$, $(a, b) = 1$, $v \geq 0$, contains an infinity of primes, and since $(1, (q - 1)) = 1$, this means that for an infinity of k in (1.95), $1 + k(q - 1)$ is prime. By (1.95) and (1.91) (c), p cannot be any of these primes. □

We see here how the fact (which followed from our assumption of a counterexample) that

$$x_c + y_c \neq z_c$$

and the fact that there exists a prime q such that $x_c + y_c$ and z_c are both $< q$, led to an infinity of facts, namely the non-congruences expressed by (1.95), which in turn gave us another infinity of facts, namely, that the prime p in the assumed counterexample could not be any of the infinity of primes required by Dirichelet's Theorem.

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 the responsibility of the present author.)

Lemma 4.0.5:
Assume a counterexample $x_c^p + y_c^p = z_c^p = 0$ *exists. Then p can be at most one prime.*

First Proof of Lemma 4.0.5

We will be using the fact that for positive numbers a and b and an exponent $r > 1$: $a^r + b^r < (a + b)^r$.

1. Let us assume there are *two* primes $p < q$ for which:
$x_c^p + y_c^p = z_c^p$;
$x_c^q + y_c^q = z_c^q$.

2. Let $(r = q/p) > 1$. By the above fact, with x_c^p and y_c^p playing the role of a and b:

$$x_c^q + y_c^q = (x_c^p)^r + (y_c^p)^r < (x_c^p + y_c^p)^r = (z_c^p)^r = z_c^q = x_c^q + y_c^q,$$

which is a contradiction. Therefore there cannot be two p which yield counterexamples for given x_c, y_c, z_c. □

Second Proof of Lemma 4.0.5:

"The Fermat curves C_m: $X^m + Y^m = 1$ intersect trivially." (A reader) □

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_c, y_c, z_c, 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_c, y_c, z_c 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 > 125,000. Or perhaps there are several prime exponents in this range, for each of which x_c, y_c, z_c 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 > 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 prime > 125,000 that is not excluded by Lemma 4.0."

An Attempted Implementation of the Approach by "Geometry of Congruences"

Our goal will be a proof by contradiction, the contradiction to arise from the congruences resulting from the assumption of a counterexample, $x^p + y^p = z^p$, and the congruences arising from known inequalities, $x^k + y^k \neq z^k$, $1 \leq k \leq p - 1$, $k \geq p + 1$. These inequalities follow from "Lemma 0.0." on page7, "Lemma 0.5." on page8, and " Lemma 4.0.5:" on page14. It is important to understand the limitation we are subject to as far as inequalities are concerned: in general, it is *not* true that if $a + b \neq c$ then $a + b$ is not $\equiv c$ mod m, for arbitrary $m \geq 2$. For example, 5 + 3 is certainly ≠ 1, but $5 + 3 \equiv 1$ mod 7. So if we want to go from inequality to guaranteed non-congruence, we must require that the modulus m be > $a, b, c, a + b$ and that $(a, m) = (b,m) = (c,m) = 1$. Under these conditions, if $a + b \neq c$ then a + b is not $\equiv c$ mod m (1.91(a)).

One way to implement our proof by contradiction, is via the concept of *towers*, which we now define.

Definition of *Tower*

Definition. Let u be any positive integer, and let $M = \{m_1, m_2, m_3, ...\}$ be an infinite sequence of moduli such that for all $i \geq 1$, $(u, m_i) = 1$, and such that $m_1 < m_2 < m_3 < ....$ Then there exists a minimum $i \geq 1$ such that $u < m_i$. In the language of "The "Lines-and-Circles" Model of Congruence" on page10, u is on level 0 mod m_i. We say that *u touches down* at m_i. Clearly, u is also < $m_{i'}$ for all $i' > i$, and so we say that *u remains down* for all these i'. ("Once u touches down, it remains down.")

By abuse of language, we will say that $u + v = w$ (or $u + v \neq w$) *touches down* at m_i when we mean that $(u, m_i) = (v, m_i) = (w, m_i) = 1$, and that u, v, and $u + v = w$ are all < m_i, and furthermore that m_i is the smallest modulus in M for which this is the case.

Definition. Assume that all the m_i in M are primes. Then if If $u^r + v^r = w^r$ touches down at m_i, and $(u, m_i) = (v, m_i) = (w, m_i) = 1$, we have, by Fermat's Little Theorem,

$$u^{(r + h(m_i - 1))} + v^{(r + h(m_i - 1))} \equiv w^{(r + h(m_i - 1))} \quad mod \ \ m_i$$

for all $h \geq 0$.

The (infinite) set of all such congruences we call a *tower mod m_i*. Similarly, if $u^r + v^r \neq w^r$ touches down at $m_{i'}$, and $(u, m_i) = (v, m_i) = (w, m_i) = 1$, we have, by Fermat’s Little Theorem,

$$u^{(r + h(m_i - 1))} + v^{(r + h(m_i - 1))} \quad is \;\; not \equiv w^{(r + h(m_i - 1))} \quad mod \;\; m_i$$

for all $h \geq 0$.

The (infinite) set of all such non-congruences we likewise call a *tower mod m_i*. In either case, we call u^r, v^r, w^r together the *base* of the tower. A congruence, or non-congruence, in a tower, we will some times call an *element* of the tower. Thus, the base of a tower forces the congruence or non-congruence of all elements of the tower.

A Possible Proof of FLT Using Towers

Let q be the smallest prime that is larger than the maximum of x, y, z (i.e., larger than z), and such that $(x, q) = (y, q) = (z, q) = 1$. By Bertrand’s Postulate, we know that $z < q \leq 2z$.

We will consider successive moduli q, q^2, q^3, ... In this case, we need to use Euler’s generalization of Fermat’s Little Theorem to build our towers. This generalization states that if $(a, m) = 1$, where m may be composite,

$$a^{\varphi(m)} \equiv 1 \quad mod \;\; m$$

Here, φ is Euler's φ function, which returns the number of numbers less than, and relatively prime to, m. It can easily be shown that if $m = q$ is prime then $\varphi(q^j) = (q - 1)q^{j-1}$, $j \geq 1$.

Let q^{j_k}, $k \geq 1$, denote the power of q at which x^k, y^k, z^k , $x^k + y^k$ all touch down, i.e., are first all less than a power of q. Then we have an infinite sequence of such powers, namely,

$$q^{j_1}, q^{j_2}, q^{j_3}, q^{j_4}\dots$$

and these give rise to the infinite sequence of statements in (1) below, all as a direct consequence of “Lemma 4.0.5:” on page14. .

(1) For all $j \geq j_1$, and for every tower element mod q^j

$$x^{1 + i \bullet \varphi(q^j)} + y^{1 + i \bullet \varphi(q^j)} is \;\; not \equiv z^{1 + i \bullet \varphi(q^j)} \quad mod \;\; q^j$$

$i \geq 0$, by “(1.91)” on page12.

And similarly for all $j \geq j_2$, all $j \geq j_3$, all $j \geq j_4$, ..., $j \geq p–1$, $j \geq p+1$, $j \geq p+2$, ..., where, of course, the exponent in the base elements of the tower in each case are 2, 3, 4, ..., p–1, p+1, p+2, ... respectively. (End of (1))

Each non-congruence element in each tower tells us that when the element touches down, it will do so as an inequality. But we already knew, from “Lemma 4.0.5:” on page14, that, for given x, y, z, only one exponent p can yield a counterexample.

Definition. Consider any tower element u in which the multiplier i in the exponent is > 1. Then any other element of the same tower with smaller i we call a *predecessor element* of u.

Assume the first element touches down at the modulus q^j and the predecessor element touches down at $q^{j'}$. Then clearly j' must be $\leq j$.

Now assume our counterexample $x^p + y^p = z^p$ touches down at q^{j_p}. There are two cases to be considered:

Case 1: the counterexample has a predecessor element in some tower mod q^{j_k}, $1 \leq k \leq p{-}1$.

Case 2: the counterexample has no predecessor element in any such tower.

Proof of the Impossibility of Case 1: there are two sub-cases to be considered:

Case 1.1: the congruence corresponding to the assumed counterexample has a predecessor element in one of the towers of *non-congruences* mod q^{j_k}, $1 \leq k \leq p - 1$.

Clearly this is impossible, because all elements of these towers are non-congruences. (The base of each tower can be regarded as an element of the tower, and the inequality in the base constitutes a non-congruence.)

Case 1.2: the congruence corresponding to the assumed counterexample has a predecessor element in some tower of *congruences* mod q^{j_k}, $1 \leq k \leq p - 1$.

But there is no such tower, since the bases of all the towers of non-congruences cover all exponents $1 \leq k \leq p{-}1$. □

Proof of the Impossibility of Case 2: If the counterexample has no predecessor element in any such tower, then for all k, $1 \leq k \leq p{-}1$, p, the exponent in our counterexample, must be $< \varphi(q^{j_k})$. But this is impossible, because then the element representing our counterexample must be at level 0 mod $q^{j_{k+1}}$, for all k, $1 \leq k \leq p{-}1$, contradicting our assumption regarding j_p.

So Case 2 is impossible. □

Hence our assumption of a counterexample leads to two impossibilities that exhaust all possibilities, and FLT is proved. (End of Possible Proof)

Approach by Induction on Inequalities

“Arithmetical” Version of the Approach by Induction on Inequalities

The reader will recall our “Vertical Approach” to a proof of FLT as described under “Brief Summary of Approaches Described in this Paper” on page5:

“[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 B.

for all k, $1 \leq k < n + 1$:
$x^k + y^k > z^k$ (Lemma 0.90);
$(x^k + y^k)/z^k > (x^{k+1} + y^{k+1})/z^{k+1}$ (Lemma 0.70).

for all $k > p = n + 1$:
$x^k + y^k < z^k$ (Lemma 0.95);
$\lim k \rightarrow \infty$, $(x^k + y^k)/z^k = 0$ (Lemma 0.97)[1].

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

We now discuss a possible proof of FLT using ratios between the FLT inequalities. We then consider the possible application of the familiar inner product from vector theory to a proof of FLT.

Strategy Using Ratios Between FLT Inequalities

We know from Lemma 0.70 that $(x^k + y^k)/z^k > (x^{k+1} + y^{k+1})/z^{k+1}$ for all k, $1 \leq k < n + 1$. It is reasonable to assume that, for each such k there exist integers a_k, b_k, with $a_k < b_k$, such that

[1] A young mathematician has written the author that Lemma 0.97 "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."

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

(We make no claim that a_k/b_k is the same for different k.)[1]

Now consider $k = n$, where $p = n + 1$ is the assumed exponent that yields a counterexample. Then it must be the case that

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

where we simply use equal signs in the exponents to show that the indicated terms all have the same value — to show that we are using several different terms to represent the same thing. We could, of course, have written, "k, which here is the same thing as p - 1, which here is the same thing as n".

But then, clearly, $(a^{k = p-1 = n})/(b^{k = p-1 = n})$ must be the reciprocal of the term it is multiplied by if the result is to be 1. Hence:

(1)

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

Since by Lemma 1.0, $x < y < z$, it is clear that the product of the numerators in the left-hand term of (1) is greater than the numerator in the center term, and similarly for the denominators. We assert that this is a contradiction, for the following reason:

We begin with two observations regarding products.

(Q)

If r, s, t are positive integers, then t is the product of r and s iff $t = rs$.

Another way of saying this is (by the Fundamental Theorem of Arithmetic),

If r, s, t are positive integers, then t is the product of r and s iff the prime factors of t (including powers) are the same as the prime factors of rs (including powers).

Now let us consider products of fractions composed of positive integers.

(Q′)

If r, s, t, u, are positive integers, then (v/w) is the product of (r/s) and (t/u) if $v = rs$ and $w = su$.

However, unlike (Q), it is *not* necessarily the case that if (v/w) = (r/s)(t/u) then (v/w) is the product of (r/s) and (t/u). For example, 1 = 7/7 = (6/3)(3/6), but 7/7 is not the product of (6/3)(3/

[1] In fact, as a reader has pointed out, given $(x^k + y^k)/z^k$,$(x^{k+1} + y^{k+1})/z^{k+1}$, then $a^k = (x^{k+1} + y^{k+1})/(x^k + y^k)$, $b^k = z^{k+1}/z^k$.

6).

We now apply (Q′) to (1), in which the product of the two fractions (r/s) and (t/u) is the left-hand term, the fraction (v/w) is the center term. Since by (1.5) under "Initial Assumptions, Definitions, and Properties of Numbers Involved" on page6 ($x, y) = (y, z) = (x, z) = 1$, and since, by Lemma 1.0, $x < y < z$, it is clear that the product of the numerators in the left-hand term of (1) is greater than the numerator in the center term, and similarly for the product of the denominators. Hence, by (Q′), the center term is not the product of the fractions in the left-hand term, which is a contradiction. (End of Strategy Using Ratios...)

Strategy Using Inner Products

The Inner Product Representation of Inequalities

$x^p + y^p \neq z^p$ can be expressed as $x^p + y^p - z^p \neq 0$, whereas a counterexample can be expressed 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 $n > 2$. 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 any ordered triple $<u, v, w>$, u, v, w integers, an *inner product term*. (An inner product term is thus a vector.)

For any inner product term $<u, v, w>$, call $<u, v, w> \bullet <1, 1, 1>$ the *value* of the term. I.e., the value of $<u, v, w>$ is simply $u + v + w$.

A Possible Strategy Utilizing Inner Products

1. Assume that $n + 1$ is the smallest exponent such that there exists x_c, y_c, z_c such that $x_c^{n+1} + y_c^{n+1} = z_c^{n+1}$.

2.By Lemma 0.90, we know that
for all k, $1 \leq k \leq n$, $x_c^k + y_c^k - z_c^k > 0$, i.e., the value of $<x_c^k, y_c^k, -z_c^k>$ is > 0.

By Lemma 0.95, we know that
for all $k' > n + 1$, $x_c^{k'} + y_c^{k'} - z_c^{k'} < 0$, i.e., the value of $<x_c^{k'}, y_c^{k'}, -z_c^{k'}>$ is < 0.

3. Let n' be any 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 0.95 we know is < 0.

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

But, as we know from Lemma 0.97 (see initial paragraphs under ""Arithmetical" Version of the Approach by Induction on Inequalities" on page 17), 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 0.95. If this is the case, we have a contradiction, and a proof of FLT.

Inner Products That Yield 0

The author assumes 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 ofFLT if one or more of these results enabled us to establish that:

$<x_c, y_c, z_c> \bullet <x_c^{n\text{-}1}, y_c^{n\text{-}1}, -z_c^{n\text{-}1}> \ > 0.$

It is well-known, of course, that, in the domain of inner product terms, unlike the domain of the reals, 0 divisors exist. Thus, e.g., $<2, 1, 0> \bullet <-1, 2, 0> = -2 + 2 + 0 = 0$, even though the value of $<2, 1, 0>$ and the value of $<\text{-}1, 2, 0>$ are both non-zero.

Inner Product Strategy Utilizing Vectors

A different strategy might be based on a fundamental result concerning the inner product, namely, that

(1) if $\mathbf{u}, \mathbf{v}$, are n-element vectors, $n \geq 1$, $\mathbf{u}, \mathbf{v} \neq \mathbf{0}$, then $\mathbf{u} \bullet \mathbf{v} = 0$ iff the angle between $\mathbf{u}$ and $\mathbf{v}$ is 90°.

Thus we can interpret FLT as asserting that it is impossible for the vectors $<x, y, z>$, and $< x^{(p\text{-}1)}, y^{(p\text{-}1)}, -z^{(p\text{-}1)}>$ to be at right angles to each other. (And similarly for the vectors $<x, y, \text{-}z>$ and $< x^{(p\text{-}1)}, y^{(p\text{-}1)}, z^{(p\text{-}1)}>$.) If we assume a counterexample, then we are asserting that every pair of vectors, $<x, y, z>$, and $< x^n, y^n, -z^n>$, $1 \leq n \leq p\text{-}2$, are not at right angles to each other, but that the vectors $<x, y, z>$, and $< x^{(p\text{-}1)}, y^{(p\text{-}1)}, -z^{(p\text{-}1)}>$, are. (And similarly for the vectors $<x, y, \text{-}z>$ and $< x^n, y^n, z^n>$, $1 \leq n \leq p\text{-}2$, and $<x, y, \text{-}z>$, and $< x^{(p\text{-}1)}, y^{(p\text{-}1)}, z^{(p\text{-}1)}>$.

The question then is, can we derive a contradiction by working with this vector representation of FLT?

“Algebraic” Version of the Approach by Induction on Inequalities

We begin by considering the following sequence S of inequalities, culminating in the assumed counterexample to the Theorem. These inequalities constitute bases of towers as described under “An Attempted Implementation of the Approach by “Geometry of Congruences”” on page 15 (the Approach in this subtitle refers to the “Geometry of Congruences”).

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

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

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

.
.
.

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

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

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:

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

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

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

...

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

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

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

We now prove two very elementary lemmas. Let:

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

Lemma 20.0
If any 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 $B_{n, (x + y)}$.

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

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

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

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

Question 4: Can this strategy[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, $a^{n-1} + a^{n-2}b + ... + ab^{n-2} + b^{n-1} = n \bullet n^{n\,-\,1}$ n^n. However, this possibility is ruled out by the constraints on x, y, z, and n. Are there any other possibilities?

"Computational" Approaches

By a "computational approach" to a proof of FLT, the author means 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?

The author believes 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

[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.

[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.

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*, accessible as downloadable PDF files 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 "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:

Given any x, y, z as possible counterexamples 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-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 "Approach by Induction on Inequalities" on page17.

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 page6, $x^p + y^p = z^p$. Then after P has computed $z^p + 0^p$, the counter C_R will show z^p incrementations. But after P has completed execution $x^p + y^p$, 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.

Our answer is simple: 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, the author 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 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.

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 any program that computes $x^p + y^p$ must always be different from the minimal length of any 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. However,

[1] by Monsur Hossain

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 bizarre sequence of machine-executable instructions that yields the desired number 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

Lemma 3.0.
Let p, q, be odd primes, and let t be any positive integer. Then there exists an infinity of primes q such that $(p, q - 1) = (t, q - 1) = 1$.

Proof[1]:

First part:

We first prove that for all $k \geq 2$, $p \bullet t$ cannot be a factor of every element of the set $S'_k = \{q_k - 1, q_{k+1} - 1, q_{k+2} - 1, \ ... \}$, where q_k is the kth prime. This implies that there exists a q_{k+h}, $h \geq 0$, such that $(p, q_{k+h} - 1) = (t, q_{k+h} - 1) = 1$.

1. Let the set S_k be all primes beginning with the kth. I.e., $S_k = \{q_k, q_{k+1}, q_{k+2}, ... \}$. Thus, e.g., if $k = 5$, then $S_k = \{11, 13, 17, 19, ... \}$, and $S'_k = \{10, 12, 16, 18, ... \}$.

Clearly, S_k contains all but a finite number of primes.

2. Now assume to the contrary that there exists a $k \geq 2$ such that, for each $h \geq 0$, $q_{k+h} - 1 = m \bullet p \bullet t$, $m \geq 1$. But then $q_{k+h} = 1 + m \bullet p \bullet t$, and thus S_{k+h} is a subset of the set $\{1 + v \bullet p \bullet t\}$, $v \geq 1$.

3. We recall that Dirichlet's celebrated Theorem asserts that every arithmetic sequence $\{a + v \bullet b\}$, $(a, b) = 1$, contains an infinity of primes. We also recall, from the theory of congruences in elementary classical number theory, that $\{a + v \bullet b\} \cap \{a' + v \bullet b\} = \phi$ if a is not congruent to a' mod b.

4. Now $\{1 + v \bullet p \bullet t\}$, $v \geq 1$, constitutes a residue class mod $p \bullet t$, and, clearly, $(1, p \bullet t) = 1$. Every prime q_{k+h}, $h \geq 0$, is in this residue class, by our assumption in step 2.

But by the second statement we recalled in step 3, none of the primes q_{k+h}, $h \geq 0$, can therefore be in the residue class $\{2 + v \bullet p \bullet t\}$, $v \geq 1$. Thus, there are only a finite number of primes in this residue class. And yet, since $(2, p \bullet t) = 1$, Dirichlet's Theorem requires that there be an infinite number of primes in this residue class.

Hence our assumption has led to a contradiction, and therefore there exists at least one q having the properties set forth in our lemma statement. □

Second part:

The fact that there exists an *infinity* of primes q having the properties set forth in our lemma statement follows directly from the fact that the first part applied to *all* $k \geq 2$ (paragraph immediately prior to step 1). That is, the first part is true no matter how large k is — in other words, no matter how large a prime we begin with in S_k. □

.

[1] This proof is an edited version of a proof by Michael O'Neill. Any errors are solely the fault of the author of this paper.

Appendix B — Lemmas Pertaining to FLT Inequalities

Lemma 0.85.
If a counterexample $x_c^{n+1} + y_c^{n+1} = z_c^{n+1}$ *exists, where* $n + 1$ *is the smallest such exponent,* then $x_c^n + y_c^n > z_c^n$.

Proof of Lemma 0.85
We use proof by contradiction.

1. Assume that

(1) $x_c^n + y_c^n > z_c^n$ *and*

(2) $x_c^{n-1} + y_c^{n-1} < z_c^{n-1}$.

(Equality is ruled out by our assumption on $n + 1$.)

2. Multiplying through (2) by z, we get

$zx_c^{n-1} + z\, y_c^{n-1} < (z\, z_c^{n-1} = z_c^{n.})$.

2. But since $z > x$, $z > y$, we have

$x^n + y^n < zx_c^{n-1} + z\, y_c^{n-1} < (z\, z_c^{n-1} = z_c^{n.}) > x^n + y^n$, a contradiction. □

Lemma 0.90.
If a counterexample $x_c^{n+1} + y_c^{n+1} = z_c^{n+1}$ *exists, where* $n + 1$ *is the smallest such exponent, then for all* k, $1 \le k \le n$, $x_c^k + y_c^k > z_c^k$.

Proof of Lemma 0.90:

1. We have already established, in Lemma 0.85, that $x_c^n + y_c^n > z_c^n$. Assume, to the contrary, that $x_c^{n-1} + y_c^{n-1} < z_c^{n-1}$ (equality is of course ruled out by our assumption that $n + 1$ is the smallest exponent in a counterexample). Is it possible that $x_c^n + y_c^n > z_c^n$?

2. $x_c^{n-1} + y_c^{n-1} < z_c^{n-1}$ implies $(x_c^{n-1} + y_c^{n-1})^{n/(n-1)} < (z_c^{n-1})^{n/(n-1)}$.

Now if the binomial theorem for exponents requires that in this case:

(I) the expansion of the left-hand side of the above inequality includes the terms $(x_c^{(n-1)})^{n/(n-1)} = x_c^n$, and

$(y_c^{(n-1)})^{n/(n-1)} = y_c^n$, and

(II) the expansion includes other terms, all positive,

then clearly $x_c^n + y_c^n < z_c^n$. Thus if $x_c^{n-1} + y_c^{n-1} < z_c^{n-1}$ it is not possible that $x_c^n + y_c^n > z_c^n$. Therefore $x_c^{n-1} + y_c^{n-1}$ must also be $> z_c^{n-1}$.

The same argument can be applied again, etc. □

Lemma 0.90 implies that $x_c + y_c > z_c$, which is confirmed by Lemma 0.0.

Lemma 0.70

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 for all k, $1 \le k < n + 1$,

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

Proof of Lemma 0.70:

1. First, assume, to the contrary, that there exists a k, $k + 1$, in the stipulated range of k such that

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

2. Multiply both sides of the equation by z^{k+1}, and get:

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

3. But $z > x$, $z > y$, and so this equation is impossible.

4. Second, assume, to the contrary, that there exists a k, $k + 1$, in the stipulated range of k such that

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

5. By the same argument as we used in steps 2 and 3, we arrive at an impossible equation. Hence we conclude that our Lemma is true. □

We now proceed to a lemma that describes the relationship between the inequalities on the "other side" of the counterexample, i.e., inequalities involving exponents $k > p = n + 1$.

Lemma 0.95.
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 for all* $k > n + 1$, $x_c^k + y_c^k < z_c^k$.

Proof of Lemma 0.95:
1. We use proof by induction.

Basis step
1. Assume that

(1) $x_c^{n+1} + y_c^{n+1} = z_c^{n+1}$.

2. Then

$(x_c^{n+1} + y_c^{n+1})^{(n+2)/(n+1)} = ((z_c^{n+1})^{(n+2)/(n+1)} = z_c^{n+2}$).

3. But then it must be the case that

$x_c^{n+2} + y_c^{n+2} < z_c^{n+2}$.

Inductive step
4. Assume that for all j, $(n + 1) < j \leq k$, $x_c^j + y_c^j < z_c^j$.

2. Then

$(x_c^k + y_c^k)^{(k+1)/(k)} < ((z_c^k)^{(k+1)/(k)} = z_c^{k+1}$).

3. But then it must be the case that

$x_c^{k+1} + y_c^{k+1} < z_c^{k+1}$. □

We can establish more regarding the ratios

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

when $k > p = n + 1$.

Lemma 0.97
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*

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

First (and Simplest) Proof of Lemma 0.97:

1. By Lemma 1.0, $x < y < z$.

2. Therefore $(x/z)^k$ can be made arbitrarily small for sufficiently large k, and similarly for $(y/z)^k$. Thus

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

□

Second Proof of Lemma 0.97:

1. If we can prove that

$$\lim_{k \to \infty} \frac{y^k + y^k}{(y+1)^k} = \left(\lim_{k \to \infty} \frac{2y^k}{y^k + \binom{k}{1} y^{k-1} + \binom{k}{2} y^{k-2} + \ldots + \binom{k}{k}} \right) = 0$$

we will have our proof of the Lemma, since the leftmost term in the leftmost equation above, in which $x = y$, and $z = (y + 1)$, is the most unfavorable case for our Lemma.

2. The first term in the denominator on the right-hand side of the leftmost equation is always y^k.

The coefficient of the second term, as is well-known, increases with increasing k, so eventually a k will be reached such that the coefficient is $\geq y$ and will remain $\geq y$ for all larger k.

So then the denominator is $\geq 2y^k$ and remains so for all larger k.

But eventually a k will be reached such that the coefficient of the second term is $\geq 2y$ and will remain $\geq 2y$ for all larger k.

So then the denominator is $\geq 3y^k$ and remains so for all larger k.

Etc. The result follows. □

Remark on Second Proof

The rate of convergence is actually faster than the above proof indicates, since we can include more terms in step 2. Thus, e.g., in the case of the coefficient of the third term, eventually an n will be reached such that the coefficient is $\geq y^2$ and will remain $\geq y^2$ for all larger k. Etc.

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.