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

Part (4)

Details on Approaches via the “Lines-and-Circles” Model of Congruence

by

Peter Schorer

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

Mar. 4, 2010

Key words: Fermat's Last Theorem

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

Definitions

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

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

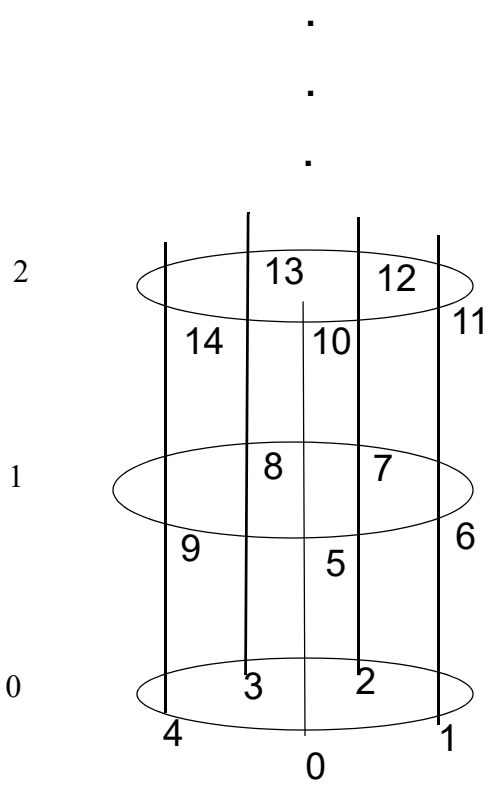

Fig. 1. "Geometrical" model of positive integers congruent mod 5.

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

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

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

(1) that, for each modulus *m*, each positive integer *u* has a "location" relative to that modulus. This location is given by the ordered pair [*level*, *line*], which can be regarded as the "address" of *u* mod *m*. Thus, in our previous example, the address of 14 mod 5 is given by [2, 4]. We will be

concerned with ordered triples $<a^k, b^k, c^k>$, where a, b, c, k are positive integers. In particular, we will be concerned with $<x^p, y^p, z^p>$, where $x^p + y^p = z^p$ is an assumed minimum counterexample, and with all $<x^k, y^k, z^k>$, where $k \geq 1$. 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."

Definition of "Appropriate Modulus"

Fermat's Little Theorem states that if p is prime, then $a \equiv a^p \bmod p$. No restriction is placed on a — that is, it is not required that $(a, p) = 1$. On the other hand, Euler's generalization of Fermat's Little Theorem states that only under the conditions that $(a, m) = 1$ is it the case that $a \equiv a^{\varphi(m)+1} \bmod m$ when m is composite. (The function $\varphi(m)$ is Euler's totient function; its value is the number of positive integers less than m and relatively prime to m. If q is a prime, then $\varphi(q) = q - 1$.) Throughout this section, therefore, when m is composite we will assume that this restriction is placed on any a, b, c — including x, y, z — that are involved in congruences mod m, and we will usually specify this by referring to m as an *appropriate modulus*.

Definition of "Congruent Ordered Triples"

Let $<a^k, b^k, c^k>$, $<a'^{k'}, b'^{k'}, c'^{k'}>$ be ordered triples, where a, b, c, a', b', c', k, k' are positive integers. Then if, for an appropriate modulus m, $a^k \equiv a'^{k'}$, $b^k \equiv b'^{k'}$, and $c^k \equiv c'^{k'} \bmod m$, we say that the *ordered triples are congruent mod m* and that $<a^k, b^k, c^k>$ *is congruent to* $<a'^{k'}, b'^{k'}, c'^{k'}>$ *mod m*. We will omit *mod m* when m is understood. For a triple $<a^k, b^k, c^k>$ there are two possibilities: $a^k + b^k \equiv c^k \bmod$ m, or $a^k + b^k$ not $\equiv c^k \bmod m$. In the first case, we say that the triple is a *congruent triple*, and in the second case we say that the triple is a *non-congruent triple*. It is important to understand that a finite or infinite set of congruent ordered triples (first sense) may contain ordered triples whose elements are congruent or non-congruent in the second sense.

Definition of a Triple Being "Below" or "Lower Than" Than Another Triple

Given two congruent triples, if each element of the first is less than the corresponding element of the second, we say that the first triple is *below*, or *lower than*, the second.

Definition of "*U*(*k*, *a*, *b*, *c*)"

Let k, a, b, c be positive integers. Then $U(k, a, b, c) = a^k + b^k - c^k$. If $x^p + y^p - z^p$ is a minimum counterexample, we often abbrieviate $U(k, x, y, z)$ to U_k .

Brief Description of Approach Type I

Details on other Approaches are given in "Appendix A — Other Supporting Material for Approaches Based on the "Lines-and-Circles" Model of Congruence" on page 5**.**

In this Approach, we try to show that the triples $<x^p, y^p, z^p>$ and $<a^k, b^k, c^k>$ give rise to a contradiction. We attempt to do this via two implementations:

First Implementation: show that the contradiction arises between $<a^k, b^k, c^k>$ that are con-

gruences but *are not* equalities, and $<a^k, b^k, c^k>$ that are congruences *and are* equalities.

Second Implementation: show that the contradiction arises from the level at which the counterexample touches down.

First Implementation

In the following, q is a prime modulus.

The Set of All Triples Below the Counterexample Triple That Are Congruences

Let S denote the set of all triples below the counterexample triple.

Let $f(d/e)$ denote the largest integer less than or equal to d/e. (Thus f is the "floor" function. It is the quotient of d divided by e.)

Then $|S|$, the number of triples below the counterexample triple, $= f(x^p/q)f(y^p/q)f(z^p/q)$.

The Set of All Triples Below the Counterexample Triple That Are Congruences <u>and</u> <u>Equalities</u>

Let $u + v = w$. Then, for the modulus q, $(u + hq) + (v + iq) = (w + jq)$ iff $h + i = j$.

Let T denote the set of all triples below the counterexample triple such that the triple is an equality.

Let $s(n)$ denote the number of 2-element partitions of n, with 0 not an element. Thus, for example, $s(5) = 4$ because $1 + 4 = 2 + 3 = 3 + 2 = 4 + 1 = 5$.

Then $|T|$, the number of triples below the counterexample triple that are equalities, is given by:

$|T| = s(z^p - q) + s(z^p - 2q) + ... + s(z^p - tq)$, where tq is the largest muliple of q such that $z^p - tq$ is positive.

The Set of All *p*-exponent Triples Below the Counterexample Triple

We define a *p-exponent triple* to be a triple $<a^p, b^p, c^p>$.

Let W = the set of all p-exponent triples below the counterexample triple.

Then $|W|$, the number of p-exponent triples below the counterexample triple, is given by:

$|W| = f(x/q)f(y/q)f(z/q)$.

If we can arrive at a contradiction among these facts, we have a proof of FLT.

Second Implementation

Let q be a prime modulus. By "Lemma 60.0:" on page 12, we know that if the triple $<a^p, b^p, c^p>$ is congruent to the triple $<x^p, y^p, z^p>$, then $a^p + b^p - c^p = U(p, a, b, c)$ is a multiple of q.

It is easily shown that in fact $U(p, a, b, c)$ is a multiple of $6q$. It follows that none of a^p, b^p, c^p is less than the modulus q — which is a strange fact, although, of course, it does not allow us to say that a^p, b^p, c^p never touch down (in our informal language, they are always "pushed up"), because for each prime modulus q, there can always be a new bottom triple.$<a^p, b^p, c^p>$. That impossibility would give us a proof of FLT. But if we can arrive at another contradiction via the strange fact, we would have a proof of FLT. For example, since, by Bertrand's Postulate (see Part (1) of this paper) there is always a prime between the prime q and $6q$, a pushing-up argument might be fashioned.

Appendix A — Other Supporting Material for Approaches Based on the "Lines-and-Circles" Model of Congruence

Original Motivation for Approaches via The "Lines-and-Circles" Model of Congruence

Two ideas originally motivated our approaches to a proof of FLT via the "Lines-and-Circles" model of congruence. The first was the following:

Assume a counterexample $x^p + y^p = z^p$ exists. Without loss of generality we can assume that $(x, y) = (y, z) = (x, z) = 1$. By Lemma 0.0 in Part (1) of this paper, we know that $x + y > z$. Therefore $x + y$ not $\equiv z \bmod p$.

But then, by Fermat's Little Theorem, $x^p + y^p$ not $\equiv z^p \bmod p$, which, since (informally) "non-congruence implies non-equality", implies $x^p + y^p \neq z^p$. This contradiction gives us a proof of FLT.

As the reader has no doubt seen immediately, there are at least two errors in this argument.

First, it is possible that one of x, y, z contains a factor p, whereas Fermat's Little Theorem requires that $(x, p) = (y, p) = (z, p) = 1$. However, it is possible that this obstacle could be overcome. (See "The Trivial Extension of Fermat's Little Theorem".)

Second, there are only two ways for $x + y > z$ to imply that $x + y$ not $\equiv z \bmod p$. One is for $x + y$ and z to be less than p. But this is impossible, since, by part (a) of Lemma 1.0, we know that $p < x$. The only other way is if w, in $x + y = z + w$, contains no factor p. But by Lemma 0.2, we know that w does contain a factor p.

The second idea that motivated our approaches via the "Lines-and-Circles" model of congruence came directly from a promising strategy for proving the $3x + 1$ Conjecture (see, for example, the paper "Are We Near a Solution to the 3x + 1 Problem?" on the web site www.occam-press.com). This strategy is called, informally, the "pushing-away" strategy. Roughly it works as follows: show that if a counterexample to the Conjecture exists, then it must be an element of the first i-level tuple of an i-level tuple-set, where $i \geq 2$. Then show that, although for each i there exists an infinity of tuples in the tuple-set that contain such a counterexample, none of these tuples ever manages to become a first i-level tuple. The candidate tuples are always "pushed away" from the first tuple position. It is then easy to show that there are no counterexample tuples, hence no counterexamples.

We had hoped to use a similar argument in the case of FLT. The argument can be simply described as follows. Suppose we are searching for a certain positive integer u. Suppose we have a series of calculations that progressively yield the *least* significant digit of u, then the least significant *two* digits of u, then the least significant *three* digits of u, etc. Suppose, furthermore, that each calculation tells us the minimum size of u.

Now suppose the calculation tells us that the smallest of all positive integers that have the correct *least* significant digit of u is greater than 10.. Suppose this calculation then tells us that the smallest of all positive integers that have the correct *two* least significant digits of u is greater than 100. And the smallest having the correct *three* least significant digits is greater than 1000, etc. It is clear that this number does not exist.

In the case of FLT, we are not looking for a single number, but for an ordered pair of numbers,

$<x^p + y^p, z^p>$, where $x^p + y^p = z^p$. We let moduli increase from 2. For each modulus m, where $(x, m) = (y, m) = (z, m) = 1$, we consider the set of all $<u^j + v^j, w^j>$, such that u^j, v^j, w^j are each less than m, and such that $(u, m) = (v, m) = (w, m) = 1$. Then by Fermat's Little Theorem, for each $<u^j + v^j, w^j>$ there are two possibilities. For all $i \geq 0$:

(1) $u^{j + i\varphi(m)} + v^{j + i\varphi(m)} \equiv w^{j + i\varphi(m)} \mod m$, or
(2) $u^{j + i\varphi(m)} + v^{j + i\varphi(m)}$ not $\equiv {}^{j + i\varphi(m)} \mod m$.

If (1) holds, then we try to show that for all i, $u^{j + i\varphi(m)} + v^{j + i\varphi(m)}$ and $w^{j + i\varphi(m)}$ cannot both be less than the next m, namely, m' such that $(x, m') = (y, m') = (z, m') = 1$. If we can show that this holds for all successive m', then we have our "pushing away" phenomenon (in this case perhaps better called "pushing up" phenomenon).

If (2) holds, then no triple $<u^{j + i\varphi(m)} + v^{j + i\varphi(m)}, w^{j + i\varphi(m}>$ can represent a counterexample, by the rule expressed informally as "non-congruence implies inequality".

We must keep in mind that, by definition of congruence, if (1) holds, then it also holds for all a, b, c congruent to u, v, w respectively mod m. And similarly for (2)

Summary of Approaches

C-sets give us a formal structure for several fundamental approaches to a proof of FLT. Each aims at a proof by contradiction. These approaches are:

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 $a \equiv x$, $b \equiv y$, $c \equiv z \mod m$.

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

(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.)

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

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

(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 $k \neq p$.

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.

Supporting Material for Approaches I - VI

The Relationship Between Congruence, Non-Congruence, Equality, and Inequality

The following basic facts relating congruence, non-congruence, equality, and inequality will be utilized throughout this paper. The proof of each is straightforward and follows directly from the definition of congruence. We supply the proof only for the lesser-known fact (2).

(1)
If $a + b = c$, then for all m, $a + b \equiv$ c mod m.
Informally: "Equality implies congruence".

(2) If $a + b \neq c$, then
(a) for an infinite number of moduli m, $a + b$ not $\equiv c$ mod m;
(b) for a finite number of moduli, it is possible that $a + b$ is not $\equiv c$ mod m or $a + b \equiv c$ mod m.
Informally: "Inequality implies non-congruence for most m; not necessarily for all."

Proof of (a):
$a + b \neq c$ implies $|c - (a + b)| = r > 0$. Then for all moduli $m > r$, there does not exist a k such that $a + b + km = c$, hence, by definition of congruence, $a + b$ not $\equiv c$ mod m.

Proof of (b):
If r is as defined in "Proof of (a)", and r is a multiple of the modulus m, then $a + b \equiv c$ mod m by definition of congruence; otherwise $a + b$ not $\equiv c$ mod m. □

Example:
If m is a modulus, and $a + b$ and c are each less than m, then $a + b$ not $\equiv c$ mod m. *(Proof:* $|c - (a + b)| < m$.. □) This case will be important throughout our development of vertical approaches via the lines-and-circles model of congruence.

(3)
If $a + b \equiv$ c mod m, then
(a) if $a + b$, c are each less than m, then $a + b = c$;
(b) if one of $a + b$, $c > m$, then $a + b \neq c$.
Informally: "Congruence implies equality for sufficiently large modulus."

(4)
If $a + b$ not $\equiv$ c mod m, then $a + b \neq c$.
Informally: "Non-congruence implies inequality."

Fermat's Little Theorem

Most of our vertical approaches that are based on congruences utilize Fermat's Little Theorem and its generalization. The Theorem states: If q is a prime then $a^q \equiv a$ mod q. Euler's generalization states: if $(a, m) = 1$ then $a^{\varphi(m)+1} \equiv a$ mod m, where m is prime or composite, and φ is Euler's totient function[1]. For a prime q, $\varphi(q) = q - 1$.

Fermat's Little Theorem implies $a^q \equiv a \bmod q$, $a^{q+1} \equiv a^2 \bmod q$, $a^{q+2} \equiv a^3 \bmod q$, ..., $a^{2q-2} \equiv a^{q-1} \bmod q$, etc. In other words, Fermat's Little Theorem implies that for $1 \leq j \leq q-1$, $a^j \equiv a^{j+k(q-1)} \bmod q$, where $k \geq 0$. Thus, for example, if $q = 5$, then $3^1 \equiv 3^5 \bmod 5$; $3^2 \equiv 3^6 \bmod 5$, etc. And similarly for Euler's generalization.

Another Fundamental Result We Will Use

In modular arithmetic, all numbers congruent to a given number (all numbers on the same vertical line as a given number in our lines-and-circles model of congruence) are equivalent. If $(a, m) = (b, m) = 1$, and $a \equiv b \bmod m$, then whatever is true modular-arithmetically of a is true modular-arithmetically of b. In particular, if $(a, m) = (b, m) = 1$, then if $a^r \equiv b \bmod m$, where $r \geq 1$, and $a \equiv c \bmod m$, then $c^r \equiv b \bmod m$. In particular, we have:

(1.91) (c)

If $(a,m) = (b,m) = (c,m) = 1$, *and if*
$a \equiv a' \bmod m$, *and* $b \equiv b' \bmod m$, *and* $c \equiv c' \bmod m$, *then*
if $a^r + b^r \equiv c^r \bmod m$, $r \geq 1$,
then $a'^r + b'^r \equiv c'^r \bmod m$ *and*
$a^r \equiv a'^r \bmod m$ *and* $b^r \equiv b'^r \bmod m$ *and* $c^r \equiv c'^r \bmod m$.
(See "(1.91) (c)" on page 6 of Part (2) of this paper, on the web site occampress.com.)

If in the above "$a^r + b^r \equiv c^r$" is replaced by "$a^r + b^r$ not $\equiv c^r$" and if "$a'^r + b'^r \equiv c'^r$" is replaced by $a'^r + b'^r$ not $\equiv c'^r$ then the resulting statement is also true.

Two Ways to Implement a Method of Infinite Descent

We assume that the reader has read the section, "Fermat's 'Method of Infinite Descent'" in Part (1). One way of implementing a Method of Infinite Descent is by using "Fermat's Little Theorem" on page 7. Suppose that q is a prime such that $(x, q) = (y, q) = (z, q) = 1$, and suppose that $p \equiv j \bmod (q-1)$, where $1 \leq j \leq q-1$ and where $p > j$. In other words, suppose $p = j + k(q-1)$, where $k > 0$. (The question whether such a q exists is discussed below in the section "Moduli" on page 9.) Then by Fermat's Little Theorem:

$x^p + y^p \equiv z^p \bmod q$ (non-congruence would imply inequality) and also
$x^{p-(q-1)} + y^{p-(q-1)} \equiv z^{p-(q-1)} \bmod q$ and
$x^{p-2(q-1)} + y^{p-2(q-1)} \equiv z^{p-2(q-1)} \bmod q$ and
...
$x^j + y^j \equiv z^j \bmod q$, where $1 \leq j \leq q-1$.

Now if we can show that the last case in the sequence is such that $x^j + y^j$ and z^j are each less than q, then we have a contradiction and hence a proof of FLT, because if $x^j + y^j \neq z^j$ then we have a contradiction, since that inequality implies non-congruence. On the other hand if $x^j + y^j = z^j$ then we also have a contradiction, namely, a counterexample whose exponent is smaller than the one in our assumed minimum counterexample $x^p + y^p = z^p$. Either contradiction gives us a proof of FLT. Is there a way that both contradictions could be avoided? Yes. Both contradictions could be avoided if, in a sequence of moduli $q^1, q^2, q^3, ..., q^k, ...$, where q^k is the first modulus such that x^p

1. $\varphi(m)$ = the number of positive integers less than m that are relatively prime to m.

$+ y^p$ and z^p are each less than q^k , at least one of $x^j + y^j$, z^j, is greater than q^j, where $1 \leq j < k$.

Another way of implementing a Method of Infinite Descent is by using "(1.91) (c)" on page 8. Here, it is the value of numbers congruent to x, y, z that are reduced, whereas in the first way it was the size of exponents congruent to p. Assume that $x^p + y^p \equiv z^p \bmod q$ (non-congruence would imply inequality). Then for all a', b' , c' such that $a' \leq x$, and $b' \leq y$, and $c' \leq z$ and such that at least one "≤" is "<", we have, by (1.91)(c) that $a'^p + b'^p \equiv c'^p \bmod q$.

Now if we can show that there exists a', b', c' such that $a'^p + b'^p$ and c'^p are each less than q, and such that at least one of a', b', $c' \neq x, y, z$ respectively, then we have a contradiction, because if $a'^p + b'^p \neq c'^p$ then we have a contradiction, since inequality implies non-congruence. On the other hand if $a'^p + b'^p = c'^p$ then we also have a contradiction, namely, a smaller counterxample (via at least one of a', b', c') than our assumed minimum counterexample $x^p + y^p = z^p$. Either contradiction gives us a proof of FLT. Both contradictions could be avoided if a similar condition prevailed as was described in the previous paragraph. This c.ondition would hold if q was such that $x + y, z$ were each less than q. In this case there would be no a', b' , c' except x, y, z.

Both ways of implementing a Method of Infinite Descent require, among other things, that a sufficiently small q exists.

Moduli

In general, we use q to denote a prime modulus, and m to denote a composite modulus whose factors are not specified.

Finding a Prime Less Than $x + y$ or z

The Vertical Approaches via the "Lines-and-Circles" Model of Congruence will make frequent use of a sequence of moduli, $q^1, q^2, q^3, ..., q^k, ...$, where q is a prime such that $(x, q) = (y, q) = (z, q) = 1$. As the reader will see, it is important that q be such that at least one of $x + y, z$ be greater than q. For a long time we believed that, because it was possible that the factors of x, y, z together could exhaust the first r primes, $r \geq 1$, the existence of such a q was in doubt. Eventually, we were able to prove that such a q exists (see "Lemma 30.0: Statement and Proof" on page 18 of Part (2) of this paper, on the web site occampress.com). For a time we thought that there was no reason to believe that a q exists that is less than y, or less than x. The reason we gave was as follows. It is possible that y is the product of all primes less than or equal to x and relatively prime to x. Furthermore, z might be the product of all the primes less than or equal to y and relatively prime to y. So the best we can hope for is that $q < z$.

But this reasoning was faulty. Let $x = 2 \cdot 3 \cdot 5 = 30$, let $y = 7 \cdot 11 = 77$, and let $z = 89$. (Our example thus conforms to the requirement of Lemma 1.0 in Part (1) that $x < y < z$ and that $x + y$ be greater than z.) Then the smallest prime q such that $(x, q) = (y, q) = (z, q) = 1$ is 13, and 13 is less than x.

The reader might immediately ask about the case $x = 2$, $y = 3$, and $z = 5$. Actually, this case and the next one are irrelevant since by 1990, prior to Wiles' proof, it was known that the exponent p in a counterexample must be larger than 125,000, and since $p < x < y < z$, there is no need to consider small numbers. Furthermore, Lemma 1.0 disallows this case because $x + y = z$ instead of the required $x + y > z$. The reader might then cite any case in which $x = 2$, arguing that there can be no prime q that is less than 2. But the case of $x = 2$ can be dismissed because, by Lemma 1.0, we know that $p < x < y < z$, and $p = 1$ is not a valid exponent in a countereexample. So there may be grounds for cautious optimism that we can prove that there exists a prime modulus q such that $(x, q) = (y, q) = (z, q) = 1$ and $q < x$.

Considering the minimum size of x, y, z, and p, it might be possible to prove that there exists a prime q such that $q < p < x < y < z$ and such that $(q, p) = (q, x) = (q, y) = (q, z) = 1$. This would immediately give us $x^k + y^k$ and z^k greater than q^k for all $k \geq 1$. Of course, for each k there exists an m such that, for all $n \geq m$, $x^k + y^k$ and z^k are each less than q^n. In other words, each pair $x^k + y^k$ and z^k must "touch down" (the term is defined below) at some modulus q^m.

If we are are able to prove that such a prime q exists, then we might have a chance of proving FLT by one of the Approaches described .

We must point out that we can take as modulus the prime exponent p in our counterexample. We know that $p < x < y < x + y$ (Lemma 1.0 in Part (1)). Taking p as modulus is discussed above in "Original Motivation for Approaches via The "Lines-and-Circles" Model of Congruence" on page 5 and in "Appendix C — Probably the Most Popular Very Simple Approach" on page 76.

We must also point out that it is not necessary for $x^k + y^k$ and z^k, where $k \neq p$, to each be less than a modulus m in order for it to follow that $x^k + y^k$ not $\equiv z^k \mod m$. For if $x^k + y^k \neq z^k$ (as is indeed the case if $k \neq p$) then $x^k + y^k + U_k = z^k$, where U_k is not 0. Then for all moduli m such that U_k is not a multiple of m, it is the case that $x^k + y^k$ not $\equiv z^k \mod m$.

Trade-offs in the Size of Moduli

It is important that we keep in mind a fundamental trade-off in the size of moduli. It is this: the larger the modulus, the fewer the number of a, b, c congruent to x, y, z and less than x, y, z. These a, b, c are the basis of several Approaches to a proof of FLT. Of course, the counterexample touches down at a sufficiently large modulus, and remains down for all larger moduli. But the larger the modulus m, the greater the chance for an a, b, c such that, for some $r > 2$, $a^r + b^r$ and c^r, are each less than the modulus. In that case, since $a^r + b^r$ cannot equal c^r, $a^r + b^r$ not $\equiv c^r \mod m$. If $a^r \equiv x^p$, $b^r \equiv y^p$, and $c^r \equiv z^p \mod m$, then we have a contradiction and a proof of FLT.

On the other hand, a small modulus m increases the chances that $m < p < x < y < z$, which is of advantage in several Approaches.

C-set — Definition

We want to capture, for each modulus m such that $(x, m) = (y, m) = (z, m) = 1$, certain ordered pairs $<a^r + b^r, c^r>$, where $(a, m) = (b, m) = (c, m) = 1$. We do this with **C**-sets. These exploit both Fermat's Little Theorem and (1.91)(c), which are described above under "Fermat's Little Theorem" on page 7 and "(1.91) (c)" on page 8. For a modulus $m \geq 2$, we define a **C**-set $\mathbf{C}_{u, v, w, j, m} \mod m$ as follows:

$\mathbf{C}_{u, v, w, j, m} = \{<u^r + v^r, w^r> \mid r \equiv j \mod \varphi(m), u^j, v^j, w^j$ are each less than m, and m is an appropriate modulus$\}$.

We say that $\mathbf{C}_{u, v, w, j, m}$ is *congruent* iff $u^j + v^j \equiv w^j \pmod m$. Otherwise $\mathbf{C}_{u, v, w, j, m}$ is *non-congruent*.

By definition of congruence, each $\mathbf{C}_{u, v, w, j, m}$ also contains all $<a^r + b^r, c^r>$ such that a, b, c are congruent to u, v, w respectively mod m.

When it is not necessary to specify a particular u, v, w, j, m, we will speak of a **C**-*set*.

Each ordered pair $<u^r + v^r, w^r>$ in a **C**-set we call an *element* of the **C**-set. The ordered pair $<u^j + v^j, w^j>$ we call the *base element* of the **C**-set. If a counterexample $x^p + y^p = z^p$ exists, we call the element $<x^p + y^p, z^p>$ the *counterexample element*. It is immediately clear that the counterex-

ample element must be an element of a congruent **C**-set. If we can show, for some modulus m, that this is not the case, then we will have a proof of FLT, because the (necessarily congruent) element $<x^p + y^p, z^p>$ is then an element of a non-congruent **C**-set, a contradiction.

It is clear that for each modulus m, the counterexample element $<x^p + y^p, z^p>$ must lie in some **C**-set mod m.

C-sets are similar to *towers* in previous versions of this paper.

Conditions for Existence of a Counterexample

We assume a counterexample $x^p + y^p = z^p$ exists, and we consider the sequence of moduli m = 2, 3, 4, ... As m increases, each $<c^p + d^p, e^p>$ will be an element of a **C**-set mod m such that $(x, m) = (y, m) = (z, m) = 1$. Here, c, d, e are each less than or equal to x, y, z respectively, and at least one of c, d, e is less than x, y, z respectively.

For each m such that $c^p + d^p$ and e^p are each less than m, the **C**-set having $<c^p + d^p, e^p>$ as base element is necessarily non-congruent because $c^p + d^p \neq e^p$. Yet it must be the case that the element $<x^p + y^p, z^p>$ is never in a non-coungruent **C**-set. So it must be that for all elements $<c^p + d^p, e^p>$ that are base elements of **C**-sets containing $<x^p + y^p, z^p>$, $c^p + d^p$ and e^p cannot each be less than m, *and, furthermore*, it must be the case that $<c^p + d^p \equiv e^p>$, since the element $<x^p + y^p, z^p>$ must always be in a congruent **C**-set *and*, *furthermore* the element $<x^p + y^p, z^p>$ must always equal an element $<u^r + v^r, w^r>$ in a congruent **C**-set, *and, furthermore*, at some m, the element $<x^p + y^p, z^p>$ must touch down.

If we can prove that no counterexample can meet all these conditions, then we have a proof of FLT.

There Are "Lots" of Non-Congruent C-sets

If a counterexample $x^p + y^p = z^p$ exists, then for all k such that $k \neq p$, $x^k + y^k \neq z^k$. Thus for all such k, $x^k + y^k = z^k + r_k$, where $r_k \neq 0$. Each r_k is the product of a finite number of prime factors. Therefore $x^k + y^k$ is not $\equiv z^k \bmod m$ for all m (an infinite number) such that r_k is not a multiple of m, regardless whether $<x^k + y^k, z^k>$ is the base element of a **C**-set or not. Furthermore, for all moduli m such that $x^k + y^k$ and z^k are both less than m, $x^k + y^k$ is not $\equiv z^k \bmod m$ (because $x^k + y^k \neq z^k$).

Thus, we would have a proof of FLT if we could show that a modulus m exists such that:

r_k is not a multiple of m;
$x^k \equiv x^p$, $y^k \equiv y^p$, $z^k \equiv z^p \bmod m$;
$(x, m) = (y, m) = (z, m) = 1$.

Furthermore, for all a, b, c, k, where $k \neq p$ and at least one of a, b, c is not equal to x, y, z respectively, it is likewise the case that $a^k + b^k \neq c^k$, and so the remarks in the previous paragraphs apply to these a, b, c, k as well.

So there are "lots" of non-congruent **C**-sets. We will have a proof of FLT if we can show that one of them contains the counterexample element $<x^p + y^p, z^p>$, because that would be a contradiction.

"Consequences" of a Counterexample

Readers who first contemplate the infinite sequence of cases,

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

sometimes react by saying, in so many words, "You have an infinite set of inequalities and exactly one equality if a counterexample exists. A counterexample is clearly a needle in a haystack! It is hopeless to try to prove (with the elementary machinery that you are using) that a counterexample exists or does not exist!"

In effect, these readers argue that the existence of a counterexample has no "consequences". The counterexample either exists or it doesn't. Everything else — all the other relationships between $a^n + b^n$ and c^n, where a, b, c are positive integers, and $n \geq 1$ — remain the same regardless.

But that is simply not true, because if $(x, q) = (y, q) = (z, q) = 1$, and q is the smallest such prime, and $x^p + y^p = z^p$, and if the counterexample element $<x^p + y^p, z^p>$ touches down at q^k (as it must, for some $k \geq 1$), then for all $k + j, j \geq 1$, $x^p + y^p \equiv z^p \bmod q^{k+j}$. The reason is that if $x^p + y^p$, z^p are each less than q^{k+j}, as must be the case ("once down, always down" (see "Definitions" on page 2)), then since $x^p + y^p = z^p$, $x^p + y^p \equiv z^p \bmod q^{k+j}$. It follows that for all moduli q^{k+j}, $<x^p + y^p, z^p>$ is the base element of a *congruent* **C**-set mod q^{k+j} . By definition of **C**-set this means that the **C**-set contains an infinity of congruent elements $<a^r + b^r, c^r>$. *None of these elements would be congruent if the counterexample did not exist*. So the existence of the counterexample definitely has "consequences".

In fact, we can say more:

Lemma 60.0:

Assume a counterexample $x^p + y^p = z^p$ exists. For all $k \geq 1$, let $U_k = x^k + y^k - z^k$. Then

(a) for each prime q, the U_k are partitioned into $q - 1$ sets, each set a proper subset of a residue class mod q. The U_k in exactly one of these sets, namely, the set containing U_p, are all multiples of q — that is, $(U_k, q) = q$.

(b) for each prime q, there is exactly one residue class mod q that contains no U_k.

(c) for each composite modulus q^j, where q is a prime, $j \geq 1$ and $(x, q) = (y, q) = (z, q) = 1$, the U_k are partitioned into $q^{j-1}(q - 1)$ sets, each set a proper subset of a residue class mod q^j. The U_k in exactly one of these sets, namely, the set containing U_p, are all multiples of q^j — that is, $(U_k, q^j) = q^j$.

(d) for each prime q, there are exactly $q - q^{j-1}(q - 1)$ residue classes mod q^j that contain no U_k..

(For proof, see "Lemma 60.0: Statement and Proof" in Part (2) of this paper, on the web site www.occampress.com.)

If $x^p + y^p = z^p$ then for all integers n, $nx^p + ny^p = nz^p$, and thus for all j, k such that $nx^p + ny^p$ and nz^p are each less than q^{k+j}, the element $<nx^p + ny^p, nz^p>$ is the base element of a **C**-set mod q^{k+j}. By definition of **C**-set this means that the **C**-set contains an infinity of congruent elements $<a^r + b^r, c^r>$. *None of these elements would be congruent if the counterexample did not exist.* So the existence of the counterexample has more "consequences".

Furthermore, since $a^r + b^r \equiv c^r \bmod q^{k+j}$ imples (by definition of congruence) that there exists a U such that $a^r + b^r + Uq^{k+j} = z^r$, it follows that for each i, where $3 \leq i < p$, there exists a U' such that $a^r + b^r + U'q^{k+j-i}q^i = c^r$, which in turn implies that $a^r + b^r \equiv c^r \bmod q^i$. This in turn implies that for each modulus q^i, where $3 \leq i < p$, there exists at least one congruent **C**-set mod q^i, namely, the one containing the element $<a^r + b^r, c^r>$.

Finally, if a counterexample exists, then for each j, k, l such that $j + k = l$ and such that each of $x^p - jm$, $y^p - km$, and $z^p - lm$ is positive, we have $(x^p - jm) + (y^p - km) = (z^p - lm)$. Each of these *equalities* occurs "below" the counterexample in the sense that each term in parentheses is less than the corresponding term in the counterexample. *These equalities would not exist if the counterexample did not exist.*

At the very least, these consequences of a counterexample should be investigated to see if they yield a proof of FLT.

An Approach Via Congruence of Exponents

Let $U_k = x^k + y^k - z^k$, where $k \geq 1$ but $k \neq p$. Then it is easy to show that, if a counterexample exists, then for each prime q, there exists a finite number of countable infinities of U_k such that each U_k does not contain the factor q, and exactly one infinity of U_k such that each U_k does contain the factor q. Furthermore, the countable infinities are disjoint. (The proof follows from the definition of **C**-set mod q, and from the definition of congruence.)

Let q be a prime and assume that k is the largest exponent such that $x^k + y^k, z^k$ are each less than q. Then each $x^j + y^j$, and z^j, where $j \leq k$, is likewise less than q. Because $x^j + y^j$, and z^j and because $x^j + y^j$, and z^j, where $j \leq k$, is likewise less than q, we know that $x^j + y^j$ not $\equiv z^j \bmod q$. *Hence* $<x^j + y^j, z^j>$ is the base element of a non-congruent **C**-set.

If there exist m, n such that $p + m(q - 1) = j + n(q - 1) = u$ for some $j \leq k$, then we have a proof of FLT, because this will imply that $x^u + y^u \equiv z^u \bmod q$ (via the **C**-set containing the counterexample) and also $x^u + y^u$ not $\equiv z^u \bmod q$ (via a non-congruent **C**-set), a contradiction. The reader should keep in mind that this argument is valid for any prime q, and that the contradiction only has to exist for one such prime. It may be that a contradiction can be forced by considering the sequence of increasing moduli each of which is a prime. In this sequence, there will be a least prime such that the counterxample is a base element. The counterexample will remain a base element for all larger primes. In addition, as the size of the primes increases, the number of base elements $<x^j + y^j, z^j>$, where $j > p$, will also increase. Perhaps this fact can force a contradiction.

We repeat: the existence of a counterexample has "consequences". Which raises the possibility of the following proof of FLT. If our assumed counterexample touches down at q^k, then all base elements of all **C**-sets in all moduli q^h, $1 \leq h < k$, are the same regardless whether or not a counterexample exists. That is, we cannot seriously imagine a professional mathematician say-

ing, 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, i.e., the difference $19^5 - (17^5 + 6^5)$ might change." Nor can we expect that the location of each element $<a^r + b^r, c^r>$ in the various **C**-sets in all moduli q^h, $1 \leq h < k$ to change. And yet the presence of these elements determines the congruence of **C**-sets whose base elements we have just said cannot change. Do we have the basis for a proof of FLT by contradiction? A topic that is closely related to that of the consequences of a counterexample will be found under part (E) of "Approach Type IV: Considering All Multiples of All Powers of a, b, c" on page 23 .

Approach Type I: Show that if $x^p + y^p = z^p$, then a contradiction arises involving $a^p + b^p$, c^p, ...

Preliminary Discussion

Elementary Fact About Equality and Congruence

Assume $a + b = c$. Then for each modulus m, and for each triple j, k, l such that $j + k = l$, there exists d, e, f such that $d + e = f$, namely, $d = a + jm$; $e = b + km$, and $f = c + lm$. (Proof: $(a + jm) + (b + km) = (a + b) + (j + k)m = c + lm$, which implies $d + e = f$.)

For example: Let a, b, c = 24, 9, 33, respectively. Then $a + b = c$ because 24 + 9 = 33. Consider the modulus 7. Then (24 – 2*7) + (9 – 1*7) = (33 – 3*7), or, 10 + 2 = 12 (d = 10, e = 2, f = 12; j = 2, k = 1, l = 3).

First Implementation

Let M denote a finite sequence of increasing appropriate moduli such that the assumed minimum counterexample $x^p + y^p = z^p$ touches down at the last modulus in the sequence. For each of the moduli m_i in the sequence, let S_i denote the set $\{<a^p + b^p, c^p> \mid a^p + b^p$ and c^p are each less than $m_i\}$. We now ask if there exist m_i and $<a^p + b^p, c^p>$ in S_i such that $a^p \equiv x^p$, $b^p \equiv y^p$, and $c^p \equiv z^p \bmod m_i$. If the answer is no, we must ask how that answer is possible, and if the answer implies a contradiction. See next paragraph. If the answer is yes, then we have a proof of FLT, for $a^p + b^p$ cannot equal c^p because in that case we would have a counterexample smaller than the minimum counterexample. So it must be that $a^p + b^p \neq c^p$ which, since $a^p + b^p$ and c^p are each less than m_i means that $a^p + b^p$ not $\equiv c^p \bmod m_i$, which implies that $x^p + y^p$ not $\equiv z^p \bmod m_i$, which is false, since $x^p + y^p = z^p$ and therefore it must be that $x^p + y^p \equiv z^p \bmod m_i$. This contradiction gives us a proof of FLT.

If the answer to the question raised in the above paragraph is no, then the following is the case: let $m_1, m_2, ..., m_i, ..., m_n$. be a sequence of appropriate moduli such that the counterexample touches down at m_n. Then for each moduli m_i in the sequence except m_n, $a^p + b^p - c^p$ is a multiple of m_i, where $a^p \equiv x^p$, $b^p \equiv y^p$, and $c^p \equiv z^p \bmod m_i$, and $a \leq x$, $b \leq y$, and $c \leq z$ (but not $a = x$, $b = y$ and $c = z$) The proof follows from a simple generalization of "Lemma 60.0:" on page 12.

We now ask if that is possible, given that the counterexample is an equality. If it isn't possible, then we have a proof of FLT. We observe that if d, e, f are each less than a modulus m, then the only possibility for a multiple of m is that $d + e - f = m$. Otherwise — for example, if d = 6, e = 6, f = 1, then d, e, and f are each less than the modulus 7, and $d + e - f$ = 6 + 6 – 1 = 11, which is not a multiple of 7. So it appears that we can say that

If a counterexample $x^p + y^p = z^p$ exists,

Then for each appropriate modulus m_i in each sequence of appropriate moduli described in the previous paragraph,

If $a^p \equiv x^p$, $b^p \equiv y^p$, and $c^p \equiv z^p \bmod m_i$, and $a \le x$, $b \le y$, and $c \le z$ (but not $a = x$, $b = y$ and $c = z$) Then either $a^p + b^p - c^p = m_i$, or else neither a^p, b^p or c^p is less than m_i.

If we can show this is false in just one case, then we have a proof of FLT.

Second Implementation

Let $x^p + y^p = z^p$ be an assumed minimum counterexample. Let m be an appropriate modulus.

We will attempt to exploit the set of equalities that is established by any equality, as we described above. The equality in our case is the counterterexample. In particular, we will attempt to arrive at a contradiction between the existence of these *equalities*, and certain congruences that are also established by the counterexample — congruences each of which must be an *inequality.*

We begin by pointing out that, for any modulus m, there is only a finite set of positive integers that are less than x^p and congruent to $x^p \bmod m$; and similarly for y^p and z^p.

The Set of Equalities

In accordance with what we said above, for each j, k, l such that $j + k = l$ and such that each of $x^p - jm$, $y^p - km$, and $z^p - lm$ is positive, we have $(x^p - jm) + (y^p - km) = (z^p - lm)$. Each of these *equalities* occurs "below" the counterexample in the sense that each term in parentheses is less than the corresponding term in the counterexample. *These equalities would not exist if the counterexample did not exist.*

First Set of Congruences

The first set of congruences, each of which represents an *inequality*, is the set $\{x^n + y^n \equiv z^n \bmod m \mid n = p - j \bullet \varphi(m)\ ,\ j \ge 1$, and n is positive$\}$. That these are congruences follows from Fermat's Little Theorem (see "Fermat's Last Theorem" in Part (4) of this paper, on the web site www.occampress.com). That each congruence is an inequality follows from "Definition of 'Minimum Counterexample'" in Part (1) "Definition of "Minimum Counterexample"" on page 15 of this Part. Each of these congruences occurs "below" the counterexample in the sense that each term in parentheses is less than the corresponding term in the counterexample.

Second Set of Congruences

The second set of congruences each of which represents an inequality is the set $\{a^p + b^p \equiv c^p \bmod m \mid a, b, c$ are less than x, y, z respectively and $a \equiv x$, $b \equiv y$, and $c \equiv z \bmod m\}$. That these are congruences follows from (1.91)(c) under "Another Fundamental Result We Will Use" in Part (4) of this paper, on the web site www.occampress.com. That each congruence is an inequality follows from "Definition of "Minimum Counterexample"" on page 15 of this Part. Each of these congruences occurs "below" the counterexample in the sense that each term in parentheses is less than the corresponding term in the counterexample. \.

If we can find a contradiction in the set of equalities and the two sets of congruences that represent inequalities, then we will have a proof of FLT. We can begin by letting m be an appropriate modulus, and then finding expressions (relative to m) for:

- the number of elements in the set S of ordered triples $<u, v, w>$ such that $u < x^p$, $v < y^p$, and $w < z^p$ and $u \equiv x^p$, $v \equiv y^p$, and $u \equiv z^p \bmod m$;
- the number of elements in the subset S_e of S consisting of ordered triples representing

equalities, including the equalities resulting from the counterexample as described above;
- the number of elements in the subset S_i of S consisting of ordered triples representing inequalities;
- the number of elements in the subset of $S_{i,c}$ of S_i consisting of ordered triples representing inequalities that are congruences mod m;
- the number of elements in the subset $S_{i,n}$ of S_i consisting of ordered triples representing inqualities that are not congruences mod m.

Two Major Obstacles in the Type I - Type III Approaches Using the Lines-and-Circles Models of Congruence

In the past we discovered what seemed to be two major obstacles to a successful proof of FLT using the Type I through Type III Approaches (see "" on page 11). Following is a brief description of each obstacle.

First Obstacle

We must assume that Lemma 30.0 (see "Lemma 30.0: Statement and Proof" on page 18 of Part (2) of this paper, on the web site occampress.com) describes a worst-case that our Approaches must deal with, unless results existing prior to 1990 show that the factors of x, y, z in a counterexample need not be all primes $\le z$. We are not aware of any such results. So we must assume that q is a prime such that x, y are each less than q, and $z > q$. [*Note*! This is not necessarily true! See "Moduli" on page 9. The reader is encouraged to read that section before reading the rest of this section.]

Now part (a) of "Lemma 1.0." on page 11 states that $p < x$. Therefore for *each set* of **C**-sets mod q such that the exponents in the base elements run from 1 through $\varphi(q)$, there exists one **C**-set whose base element is $<u^p + v^p, w^p>$. The reason is that $p < x < q$ implies $p < \varphi(q) = q - 1$. In other words, for each u, v, w such that u, v, w, $< q$ and $(u, q) = (v, q) = (w, q) = 1$, there exists a base element of a **C**-set in which the exponent of u, v, w is p.

In some cases, for the base element $<u^p + v^p, w^p>$, it will be the case that $u^p = x^p$, $v^p = y^p$, since x, y, $< q$. But z^p cannot be the second term of a base element since $z > q$ and hence cannot equal w in a base element, by definition.

So if $z > q$ (it can easily be shown that $q < z < 2q$), then $z \equiv w \bmod q$, where $w < q$ and we have $x^p + y^p \equiv w^p \bmod q$ (by "(1.91) (c)" on page 6 of Part (2) of this paper, on the web site occampress.com). Since by assumption $x^p + y^p = z^p$, we also have $x^p + y^p \equiv z^p \bmod q$. But this does not do us any good. And because x, $y < q$, and $z > q$ we cannot use either Fermat's Little Theorem or (1.91)(c) to arrive at a contradiction as our modulus increases to q^2, q^3, ...

Second Obstacle

The second obstacle is also related to the fact that $p < x$. This fact means that if the modulus q is greater than x, then $<x^p + y^p, z^p>$ is *always* the base element of each **C**-set mod q^k, where $k \ge 1$, in which it is an element. The reason is that since, as is well-known, $\varphi(q^k) = (q - 1)q^{k-1}$, it follows that $p - \varphi(q^k)$ is negative. Thus, if $n = p - j(\varphi(q^k))$, where $j \ge 1$, there cannot be an element $<x^n + y^n, z^n>$ in a **C**-set mod q^k. Thus our hope of proving that $<x^p + y^p, z^p>$ is an element of a non-congruent **C**-set, and from this contradiction obtaining a proof of FLT, appears to be in vain.

First Attempt to Overcome the First Obstacle in the Type I - Type III Approaches

At the modulus q^2, $z < q^2$ and so $<x + y, z>$ is the base element of a **C**-set. In the set of **C**-sets mod q^2 such that the base elements are $<x^j + y^j, z^j>$, where $1 \le j \le \varphi(q^2)$, there exists one **C**-set whose base element is $<x^p + y^p, z^p>$, since if $p < x < q$ then $p < \varphi(q^2) = q(q - 1)$.

The **C**-set whose base element is $<x^p + y^p, z^p>$ must be congruent because (informally) non-congruence implies inequality, contradicting our assumption that $x^p + y^p = z^p$.

By definition of **C**-set there is an infinity of a, b, c such that $a^r + b^r \equiv c^r \bmod q^2$, where $a \equiv x$, $b \equiv y$, $c \equiv z \bmod q^2$, and $r \equiv p \bmod \varphi(q^2)$. (These congruences would not exist if our assumed counterexample did not exist. They are examples of the "consequences" of the existence of a counterexample described under ""Consequences" of a Counterexample" on page 11.)

By definition of congruence, this means that for each a, b, c, r, there exists an h such that $a^r + b^r + hq^2 = c^r$. Because there can be only one counterexample with exponent p, it follows that $h \neq 0$.

We observe in passing that there are two possible types of inequality for $a^r + b^r$, c^r relative to a modulus q^k, where $k \ge 1$. The first type is that in which $a^r + b^r + h = c^r$ and h is not a multiple of q^k (in other words, in which $a^r + b^r$ is not $\equiv c^r \bmod q^k$, hence $a^r + b^r \neq c^r$) and the second type is that in which h *is* a multiple of q^k (in other words, in which $a^r + b^r \equiv c^r \bmod q^k$ even though $a^r + b^r \neq c^r$) .

Second Attempt to Overcome the First Obstacle in the Type I - Type III Approaches

We begin our Second Attempt by recalling a fact from elementary number theory, namely, that if $(a, m) = 1$, then the sequence $1a$, $2a$, $3a$, ..., ma, contains the set of all residue classes mod m in some order. If the sequence continues — $(m + 1)a$, $(m + 2)a$, ..., $2m(a)$ — then the order of residue classes repeats, etc.

Let q be the modulus defined above under "Two Major Obstacles in the Type I - Type III Approaches Using the Lines-and-Circles Models of Congruence" on page 16 and let k be ≥ 1. Then $<x^p + y^p, z^p>$ is an element (not necessarily the base element) of a congruent **C**-set mod q^k. Now consider the sequence of elements,

(1)
$<1x^p + 1y^p,\ 1z^p>$
$<2x^p + 2y^p,\ 2z^p>$
$<3x^p + 3y^p,\ 3z^p>$
...
$<q^k x^p + q^k y^p,\ q^k z^p>$.

The multiples of $x^p + y^p$ will cover all residue classes mod q^k, and similarly for the multiples of z^p. If this implied that for each **C**-set mod q^k, there existed an n such that $<nx^p + ny^p,\ nz^p>$ were an element of the **C**-set, then we would have a proof of FLT, because we would have shown that all **C**-sets mod q^k must be congruent, contrary to the fact that, for sufficiently large k, there exist **C**-sets that are not congruent, namely, those **C**-sets having base element $<x^j + y^j, z^j>$, where $j \ge 1$, $j \neq p$, and $x^j + y^j$ and z^j are each less than q^k. In these cases, the base element $<x^j + y^j, z^j>$ must be non-congruent because $x^j + y^j \neq z^j$, hence, since $x^j + y^j$ and z^j are each less than q^k, $x^j + y^j$ is not $\equiv z^j \bmod q^k$. Hence the **C**-set is non-congruent.

Unfortunately, the first and second terms in the elements of sequence (1) cannot possibly cover the set of all *pairs* of residue classes mod q^k of which there are $\varphi(q^k)\varphi(q^k)$. So we must uti-

lize the known non-congruent **C**-sets . These *include* the ones having base element $< u^j + v^j, w^j >$, where $1 \leq j \leq \varphi(q^k)$, and where $u^j + v^j$ is not $\equiv w^j \bmod q^k$. Such a non-congruence is guaranteed to occur if $u^j + v^j$ and w^j are each less than q^k and $u^j + v^j \neq w^j$.

For each such non-congruence, we get a sequence of elements similar to that in (1), except here each element represents a non-congruence.

Our goal now is to show that (informally) there is not sufficient "room" in the set of all **C**-sets mod q^k, for the congruences in (1) to exist. The reader should keep in mind that as q^k increases beyond the value at which the counterexample touches down, the number of base elements $< x^j + y^j, z^j >$, where $j \neq p$, and $x^j + y^j$ and z^j are each less than q^k, so that $x^j + y^j$ is not $\equiv z^j \bmod q^k$ — the number of these base elements increases. For each of these base elements, there is a countable infinity of inequalities via our multiples by all n. Each of these inequalities eventually touches down. But there is only one countable infinity of inequalities for our base element $< x^p + y^p, z^p >$.

Remark on Second Attempt

If we apply to the Second Attempt the question recommended under "The Danger of 'Null' Approaches in Part (1), "Does this approach or strategy apply to all a, b, c such that $a + b$ = c?", it is hard to avoid the conclusion that the answer is yes. And so we must at least tentatively declare the Second Attempt unpromising.

Third Attempt to Overcome the First Obstacle in the Type I - Type III Approaches

The major obstacle in the Type I - Type III approaches is due to the fact that we must have $(x, q) = (y, q) = (z, q) = 1$ and that the prime q must be sufficiently small. It takes considerable effort just to prove that there exists q such that $(x, q) = (y, q) = (z, q) = 1$ and $z > q$ (see "Lemma 30.0: Statement and Proof" on page 18 of Part (2) of this paper, on the web site occampress.com.). But if we allow one of x, y, z to have a factor in common with q, then at least conceptually things become much simpler. For in this case, we can choose q to be as small as we like, namely, to be any prime greater than or equal to 2, thus assuring us that the counterexample $<x^p + y^p, z^p>$ is very high up in the lines-and-circles model for q. We might then be able to invoke "(1.91) (c)" on page 6 of Part (2) of this paper, on the web site occampress.com, and show that there exist a, b, c such that $a^p + b^p \equiv c^p \bmod q$ and $a^p + b^p$ and c^p are each less than q, so that $a^p + b^p = c^p$, contrary to our assumption that $x^p + y^p = z^p$ is the minimum counterexample. But, of course, we must first show that allowing one of x, y, z to have a factor in common with q does not defeat our purpose.

Only recently did it occur to us that it may not be necessary to find a, b, c such that $a^p + b^p$ and c^p are each less than q. The reason we have always assumed it was necessary was that if $a^p + b^p \equiv c^p \bmod q$ and $a^p + b^p$ and c^p are each less than q, then we can be sure that $a^p + b^p = c^p$, thus giving us our contradiction. But we must ask if it is not possible that we might be able to find an a, b, c such that $a^p + b^p \equiv c^p \bmod q$ implies $a^p + b^p = c^p$ without both $a^p + b^p$ and c^p being less than q.

Consider the integers mod 7, and consider the case of <16 + 17, 33>. It is true that 16+ 17 = 33, and therefore that $16 + 17 \equiv 33 \bmod 7$. It is also true that $16 \equiv 9 \bmod 7$, $17 \equiv 10 \bmod 7$, $33 \equiv 19 \bmod 7$, $9 + 10 \equiv 19 \bmod 7$, and that *9 + 10 = 19*, even though 9 + 10 and 19 are each greater than the modulus 7.

Let us return to FLT. We have $x^p + y^p \equiv z^p \bmod q$ because $x^p + y^p = z^p$. We ask if there exist a, b, c such that:

at least one of a, b, c differs from x, y, z respectively, and
$a \equiv x$, $b \equiv y$, and $c \equiv z \bmod q$, and

$a^p + b^p \equiv c^p \bmod q$ and
$a^p + b^p = c^p$.

That is, we ask, by definition of congruence, if there exist u, v, w not all 0 such that

$$(x + uq)^p + (y + vq)^p = (z + wp)^p + 0q. \quad (1)$$

Unfortunately, one set of values for u, v, w gives us a trivial result. Namely, if $u = x$, $v = y$, and $w = z$, then (1) is true, but it is equivalent to

$$x^p(1 + q)^p + y^p (1 + q)^p = z^p(1 + q)^p + 0q,$$

in other words, it is equivalent to a mere multiple of (1)

A Major Obstacle in the Type III and V Approaches Using the Lines-and-Circles Models of Congruence

Let us expand our definition of **C**-set so that for each u, v, w such that u, v, w are each less than the modulus m, and such that $(u, m) = (v, m) = (w, m) = 1$ there is a **C**-set for each $<u^k + v^k, w^k>$, where $1 \le k \le \varphi(m)$. Now let u, v, $w = x$, y, z respectively. Then we will have a proof of FLT if we can show that an m exists such that, for each k, where $1 \le k \le \varphi(m)$, the **C**-set containing $<x^k + y^k, z^k>$ is non-congruent. For the counterexample element $<x^p + y^p, z^p>$ must be in one of these **C**-sets, and since the element is congruent, we have our contradiction.

The major obstacle is that there seems no way of proving that such an m exists. In particular, if $<x^p + y^p, z^p>$ is always the base element of one of the **C**-sets in our set, then we have no contradiction.

The key question is, can we find (Condition (1)) an appropriate modulus m such that $p \le \varphi(m)$. If so, then we must see if (Condition (2)) all the **C**-sets in the above set are non-congruent. If they are, then we have our contradiction and our proof of FLT.

We can begin our inquiry with $m = 3$. We see immediately that $\varphi(3) = 2$. As of the early nineties, p was known to be greater than 125,000, so our first condition is easily met. The problem is that $m = 3$ requires that neither x, y, or z have a factor of 3. (For the time being we ignore possible use of the Trivial Extension to Fermat's Little Theorem.). We can compute the largest modulus m_{max} such that $\varphi(m_{max})$ is less than 125,000. Then FLT is true for all x, y, z such that $(x, m) = (y, m) = (z, m) = 1$, where $m \le m_{max}$, and all the **C**-sets in the above set are non-congruent.

Approach Type III: Finding a Non-Congruence in a Congruent C-set

To review: In this Approach, we assume a counterexample exists. For a sufficiently small prime q we define a succession of moduli, q, q^2, q^3, q^4, ... , q^k, ... We represent each modulus by a lines-and-circles model as defined above. We then impose upon each such model a set of "towers" of tuples $<a^r + b^r, c^r>$ that are congruent in a sense that is made precise. These "towers" are called "**C**-sets". In a **C**-set, we have either that, for all tuples, the first element of each tuple is congruent to the second, or that, for all tuples, the first element of each tuple is not congruent to the second. In the first case, the **C**-set is said to be "congruent", in the second case "non-congruent."

For each modulus, one **C**-set (necessarily congruent) contains our assumed counterexample in the tuple $<x^p + y^p, z^p>$. The tuples "touch down" at the base level of sufficiently large q^k, that

is, at the modulus q^k such that $a^r + b^r$ and c^r are each less than q^k. At the base level either $a^r + b^r = c^r$ or $a^r + b^r \neq c^r$. We attempt to use this wealth of **C**-sets and the touching-down phenomenon to show that a counterexample tuple is an element of a non-congruent **C**-set, which is a contradiction, and thus gives us a proof of FLT.

First Implementation

A possible way to overcome the above-mentioned obstacles is the following. We remind the reader that, as of 1990, prior to Wiles' proof, p was known to be greater than 125,000, and that if a number u is a product of the first m primes (as x, y, or z might be), where $m > 2$, there are primes less than u and relatively prime to u. For example, if $u = (2)(3)(5)(7)(11)$, then, for example, $(u, 13) = 1$ and $13 < u$. We now state conditions for a simple proof of FLT.

Conditions for the Truth of FLT

If there exists a prime q such that:

(1)
$q < p < x < y < z$ and
$(x, q) = (y, q) = (z, q) = 1$ (obviously $(p, q) = 1$) and
for some k, where $1 \leq k < \varphi(q) = q - 1$ it is the case that
$k \equiv p \bmod q - 1$ and
$x^k \equiv x^p \bmod q$,
$y^k \equiv y^p \bmod q$,
$z^k \equiv z^p \bmod q$, and
$(U_k, q) = 1$, implying that $x^k + y^k$ not $\equiv z^k \bmod q$,
where $x^k + y^k - U_k = z^k$ and $U_k \neq 0$ because $x^k + y^k \neq z^k$,

then FLT is true.

Proof:

For each positive integer n (including $n = p$), there exists a k, $1 \leq k < q - 1$ such that $n \equiv k \bmod (q - 1)$ (by Fermat's Little Theorem). But since $q < p < x < y < z$, $x^p + y^p$ and z^p are greater than $x^k + y^k$ and z^k, respectively, for each k, where $1 \leq k < q - 1$. Since, for the k specified in the above conditions, $x^k + y^k$ not $\equiv z^k \bmod q$, it follows that $x^p + y^p$ not $\equiv z^p$, a contradiction. Thus FLT is proved.

Discussion

The conditions (1) can be weakened so as not to require that $(x, q) = (y, q) = (z, q) = 1$. Furthermore, by Fermat's Little Theorem, if $j \equiv h \bmod q - 1$, then for each u, v, $u^j \equiv v^h \bmod q$, and so we can eliminate the explicit listing of the conditions $x^k \equiv x^p \bmod q$, $y^k \equiv y^p \bmod q$, and $z^k \equiv z^p \bmod q$. Thus, without loss of generality, the conditions for the truth of FLT can be reduced to:

If there exists a prime q such that:

$q < p < x < y < z$ and
for some k, where $1 \leq k < \varphi(q) = q - 1$ it is the case that
$k \equiv p \bmod q - 1$ and

$(U_k, q) = 1$, implying that $x^k + y^k$ not $\equiv z^k \bmod q$,
where $x^k + y^k - U_k = z^k$ and $U_k \neq 0$ because $x^k + y^k \neq z^k$,

then FLT is true.

(2) We know, by "Lemma 1.5." on page 11, that for each k, where $1 \leq k < p$, $x^k + y^k - z^k = U_k < x^k$. For each k, U_k is fixed, since x, y, z are fixed — that is, U_k is not a function of the modulus q^k. If we can show that there exists just one q such that the conditions in the above antecedent are fulfilled, we will have a proof of FLT. One way of showing this is to show that the number of primes in U_k is less than the number of eligible q. Another way is via the "The "Smaller Prime" Lemma" on page 14.

A Simple Implementation of the Vertical Approach Based on Congruences

Let q be a prime such that:

$q < p < x < y < z$ and
for all k, where $1 \leq k < \varphi(q) = q - 1$ it is the case that
$(U_k, q) = 1$, where $x^k + y^k = z^k + U_k$ ($U_k \neq 0$ because $x^k + y^k \neq z^k$),
implying that $x^k + y^k$ not $\equiv z^k \bmod q$.

Then FLT is true.

The proof is the same as that given under "Conditions for the Truth of FLT" on page 20. Since $q < p$, it is clear that x^p, y^p and z^p are each greater than x^{q-1}, y^{q-1}, and z^{q-1}. "Fermat's Little Theorem" on page 7 allows x, y, and z to have a factor q, although, since $(x, y) = (y, z) = (x, z) = 1$, only at most one of x, y, z will have that factor. We conjecture that "The "Smaller Prime" Lemma" on page 14 will enable us to prove the existence of the desired prime q. We remind the reader that, as of 1990, prior to Wiles' proof of FLT, the prime p was known to be greater than 125,00. Furthermore, by part (g) of "Lemma 1.5." on page 11, each U_k is a multiple of p, which is in our favor, since by "The "Smaller Prime" Lemma" on page 14, this increases the number of primes less than, and relatively prime to U_k.

An Even Simpler Implementation of the Vertical Approach Based on Congruences

Let U_k be defined as in the previous sub-section. Let q be the smallest prime such that $(U_1, q) = (U_2, q) = ... = (U_{q-1}, q) = 1$. Such a prime exists, because there are only a finite number of primes in all these U_k.

But then, if $p > q - 1$, it follows, by what we established under "C-set — Definition" on page 10, that $x^p + y^p$ not $\equiv z^p \bmod q$, which is not possible if $x^p + y^p = z^p$. Hence we would have a prove of FLT.

We can weaken considerably our constraints on the U_k and still achieve our goal. For, if there exists a prime q such that (1) $p > q - 1$, and (2) $(U_k, q) = 1$, where

$x^k \equiv x^p \bmod q$,
$y^k \equiv y^p \bmod q$, and

$z^k \equiv z^p \bmod q$,

then it follows, by what we established under "C-set — Definition" on page 10), that $x^p + y^p$ not $\equiv z^p \bmod q$, which is not possible if $x^p + y^p = z^p$. Hence we would have a prove of FLT.

We can describe a procedure for searching for the impossibility.

1. Compute $U_1, U_2, U_3, ..., U_{q-1}$, where q is the largest prime $< p$. We have now computed $U_1, U_2, U_3, ..., U_{q'-1}$, for each prime $q' < p$.

2. Beginning with $q' = 2$, find the k such that

$x^k \equiv x^p \bmod q$,
$y^k \equiv y^p \bmod q$, and
$z^k \equiv z^p \bmod q$.

By "Fermat's Little Theorem" on page 7, we know that such a k must exist. If $(U_k, q') = 1$, then we have a proof of FLT. If $(U_k, q') \neq 1$,, then repeat step 2 for the next q' in the sequence. Of course, if we do not find a U_k such that $(U_k, q') = 1$, then our strategy has failed.

The insightful reader will point out that the chances of our strategy succeeding are reduced if each U_k is a single, different prime less than q. Although "Lemma 0.2" on page 10 shows that for each k, $U_k > 2 \bullet 3 \bullet 5 \bullet p$ we cannot regard this as encouragement that our strategy might succeed. For Fermat's Little Theorem and the definition of congruence imply that for each prime q', the crucial U_k *must* be a multiple of q', thus depriving us of the needed contradiction.

We continue now with the discussion we were engaged in prior to the details of these two simple Approaches:

(3) If, in attempting to prove that $(U_k, q) = 1$, we assume the contrary, then we have

$x^k + y^k - z^k \equiv x^p + y^p - z^p \bmod q$,

which, by definition of congruence implies there exists a term qR such that

(2)
$x^k + y^k - z^k - qR = x^p + y^p - z^p$.

R must be positive because, by "Lemma 1.5." on page 11, $x^k + y^k - z^k$ is positive, whereas the right-hand side of equation (2)= 0. We know that U_k must be positive for the same reason, so equation (2) becomes

$U_k - qR = 0$.

If we factor the largest power of q out of each term, yielding

$q^h M - q^j N = 0$

we see immediately that h must equal j in order to avoid a contradiction. This seems rather fortuitous, since $U_k = q^h M$ is fixed, and not a function of any modulus. So we have at least some encouragement for trying to find a q' having no factors in common with U_k. A strategy that is based on considerations of the prime factors of each U_k is given under "Approach Type VI: Show that the Assumption of a Counterexample Implies a Contradiction in the U_k" on page 27..

Second Implementation

The vast majority of our attempts at a proof of FLT using vertical approaches based on congruences rely on the application of Fermat's Little Theorem to the exponents in ordered pairs $<u^r + v^r, w^r>$. However, we can also apply "(1.91) (c)" on page 8, namely, we can hold the exponent p fixed and investigate ordered pairs $<a^p + b^p, c^p>$ which are congruent, as defined for **C**-sets, to the counterexample ordered pair $<x^p + y^p, z^p>$.

In order to fix ideas, we begin by considering any positive integers d, e, f, such that $d + e = f$. This equality is not affected by the modulus m in which the numbers are represented. If at least one of the pair $d + e$ and f is greater than m, then there will be $h + i$ and j, each of the pair less than m, such that $d \equiv h$, $e \equiv i$, and $f \equiv j \bmod m$ and such that $h + i = j$. For example, consider the equality $25 + 15 = 40$. We find that $25 \equiv 3$, $15 \equiv 4$, and $40 \equiv 7 \bmod 11$, that each of $3 + 4$ and 7 are less than 11, and that indeed $3 + 4 = 7$.

Now consider the counterexample equality $x^p + y^p = z^p$ and an appropriate modulus m such that at least one of the pair $x^p + y^p$ and z^p is greater than m. Then there will be $r + s$ and t, each less than m, such that $x^p \equiv r$, $y^p \equiv s$, and $z^p \equiv t \bmod m$ and such that $r + s = t$. What cannot be the case is that $r = a^p$, $s = b^p$, and $t = c^p$, for positive integers a, b, c, because that would imply two counterexamples with the same exponent p, which is not allowed by "Lemma 4.0.5" on page 13.

But "(1.91) (c)" on page 8 guarantees us that for each $a \equiv x$, $b \equiv y$, and $c \equiv z \bmod m$, including those a, b, c such that $a + b$ and c are each less than m, it is the case that $a^p + b^p \equiv c^p \bmod m$. So to avoid a contradiction, at least one of $a^p + b^p$, c^p must be greater than m, and this must always be the case for all appropriate moduli m such that at least one of the pair $x^p + y^p$ and z^p is greater than m. If we can show that this is impossible, then we will have a proof of FLT. We point out two things: (1) that for each a, b, c, there exists an infinity of moduli m such that $a^p + b^p$ and c^p are each less than m, and (2) that by Fermat's Little Theorem, if $a^p + b^p \equiv c^p \bmod m$, then $a + b \equiv c \bmod m$.

Approach Type IV: Considering All Multiples of All Powers of *a, b, c*

The motivation for this Approach is the sub-section ""Consequences" of a Counterexample" on page 11. In brief, and informally, we ask: if the existence of a counterexample, $x^p + y^p = z^p$, implies the existence of an infinity of equalities, $nx^p + ny^p = nz^p$, where n is a positive integer, is it possible that there is not enough "room" for all these equalities which, if no counterexample existed, would be inequalities?

We list a set of facts, inviting the reader to apply his or her creativity to possibly coming up with a proof of FLT from them. The letters (A), (B), (C), etc. are merely for the purpose of reference, and are not intended to imply that the facts they designate are steps in a logical argument.

(A) Assume that a, b, c are positive integers and that $a + b = c$. Without loss of generality, we can write $a = nf$, $b = ng$, $c = nh$, where n is a positive integer. There are now two possibilities: (I)

$n = 1$, and (II) $n > 1$. Case (I) can be broken down into two further cases: (I.1): f, g, h are powers of the same exponent; (I.2): f, g, h are powers of different exponents.

(B) Similarly, assume that a', b' and c' are positive integers and that $a' + b' \neq c'$. Without loss of generality, we can write $a' = nf'$, $b' = ng'$, $c' = nh'$, where n is a positive integer. There are now two possibilities: (I) $n = 1$, and (II) $n > 1$. Case (I′) can be broken down into two further cases: (I′.1): f', g', h' are powers of the same exponent; (I′.2): f', g', h' are powers of different exponents.

(C) Let u, m be positive integers, and let $(u, m) = 1$. Consider the infinite sequence of congruences,

$1u \equiv a_1 \bmod m$;
$2u \equiv a_2 \bmod m$;
$3u \equiv a_3 \bmod m$;
...
$mu \equiv a_m \bmod m$;
$(m + 1)u \equiv a_{m+1} \bmod m$;
$(m + 2)u \equiv a_{m+2} \bmod m$;
$(m + 3)u \equiv a_{m+1} \bmod m$;
...
where the a_i are minimum residues mod m.
Then by a basic fact of congruence theory, $a_1, a_2, a_3, \ldots, a_m$ is a sequence of all m minimum residues mod m. Furthermore $a_{m+1} = a_1, a_{m+2} = a_2, a_{m+3} = a_3$, etc.

We see immediately that if a counterexample exists, and $(x, m) = (y, m) = (z, m) = 1$, then in *each* residue class mod m there exists an infinity of pairs $<nx^p + ny^p, nz^p>$, where n is a positive integer.

(D) If x, y, z are constituents of a counterexample, then by "Lemma 0.0" on page 10, $x + y > z$. It follows from (B) that

(1)
$1x + 1y > 1z$;
$2x + 2y > 2z$;
$3x + 3y > 3z$;
...
$n\mathrm{x} + n\mathrm{y} > nz$;
...
By "Lemma 0.2" on page 10, we know that $x + y = z + Kdef$, and so we can write, from (1),

(2)
$1x + 1y = 1z + 1Kdef$;
$2x + 2y = 2z + 2Kdef$;
$3x + 3y = 3z + 3Kdef$;
...
$n\mathrm{x} + n\mathrm{y} = nz + nKdef$;

...

(E) Consider a 5-dimensional matrix M such that cell (n, u, v, w, k) is occupied by the value of $nu^k + nv^k - nw^k$, where n, 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 cell — if we know n, u, v, w, k, then we can compute the value of $nu^k + nv^k - nw^k$, and then *from that value* we can compute the value of, for example, $n(u-1)^k + nv^k - nw^k$, which is the value of one of the cells next to that containing $nu^k + nv^k - nw^k$. In fact, there are 10 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 fact that the value of the contents of cells adjacent to a given cell can be computed *from the value* of that cell *is important*! Let us give an example.

Consider the cell at (x, y, z, p) which, by definition of the value of a cell, and by assumption of a counterexample, contains $x^p + y^p - z^p = 0$. A neighboring cell at $(x, y-1, z, p)$ contains the value $x^p + (y-1)^p - z^p$. But for all values of $x^p + y^p - z^p$ we have

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

Clearly, given that x, y, z are fixed, the value of $x^p + y^p - z^p$ determines the value of $x^p + (y-1)^p - z^p$.

This fact forces us to consider the following. We begin with a quote from the section,""Consequences" of a Counterexample" on page 11): "...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, i.e., the difference $19^5 - (17^5 + 6^5)$ might change." In terms of our matrix, we say that the contents of certain cells would remain unchanged regardless if FLT were proved or if a counterexample were discovered. And yet, as we have shown in that section, an infinity of cells would have different contents if a counterexample existed — different from what they would have if FLT were true. So we ask: where is the "dividing surface" in the matrix M between cells whose contents would remain unchanged, and cells whose contents would be changed by a counterexample? Prior to 1990 it was known that if a counterexample existed, p would be greater than 125,000 and (therefore, since $p < x$ by "Lemma 1.0." on page 11) x would be greater than p. So all cells whose coordinates included p less than or equal to 125,000, would have permanent contents, regardless if a proof of FLT or counterexamples were later discovered. Is it in the nature of a counterexample that somehow, from beyond a few cells of the counterexample, the contents of all cells remains the same as they would be if counterexamples did not exist?

The matrix provides a framework for mathematical induction on any coordinate. 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 contents 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.

The matrix is the second "geometric" representation of a number-theoretic relation we have introduced in this paper, the first having been the lines-and-circles model of congruence (see under "Approaches via The "Lines-and-Circles" Model of Congruence" on page 15).

We note immediately that if a counterexample exists, then M has an infinity of cells containing 0 that would *not* contain 0 if a counterexample did not exist. There is one of these cells (n, x, y, z, p) for each n. There is another countable infinity of cells containing values that would be different from those it would have if a counterexample did not exist. These are the cells representing congruences in **C**-sets whose base element is $<x^p + y^p, z^p>$. See ""Consequences" of a Counterexample" on page 11.

Does the multi-dimensional matrix concept, as applied above, provide us with a means of proving that no cell contains the value 0 if $k > 2$? It may be profitable to consider two or more different "paths" — two or more different sequences of adjacent cells — from the cell (1, x, y, z, p) to, say, the cell (1, x , y, z, ($p - 1$)). If the end value of different paths is not the same, then we have a contradiction and hence a proof of FLT.

To begin our investigations, let us consider the cell (1, x, y, z, p), whose value, by our assumption of a counterexample, is 0. Does the adjacent cell (1, ($x - 1$), y, z, p) contain a negative or a positive value? We see immediately that it contains a negative value, because $(x-1)^p + y^p - z^p + (x^p - (x-1)^p) = x^p + y^p - z^p = 0$, and $(x^p - (x-1)^p)$ is positive. Informally, if we had a positive number b to a number a and get zero, then a must be negative.

We conclude that the cell (1, ($x - 1$), ($y - 1$), z, p) contains a more negative number than (1, ($x - 1$), y, z, p).

Conjecture: if $u > 125{,}000$ and $p < u$, then $(u-1)^p > u^{(p-1)}$.

Recalling that, by part (g) of "Lemma 1.5." on page 11, $x^{p-1} + y^{p-1} - z^{p-1} \geq Kdef + p - 2$, we ask if our Conjecture, if true, implies a contradiction.

Approach Type V: Considering Congruences and Non-congruences Resulting from All C-set Pairs

Let M denote the set of all moduli m such that there exist **C**-sets mod m. Let the elements of M be placed in a non-decreasing order: m_1, m_2, m_3, ...

Let $U = \{u_k \mid x^k + y^k + u_k = z^k, \text{ for } k \geq 1\}$.

Now consider the following table:

Table 1: Relating Certain Congruent Elements of C-sets, and Moduli

u_k	m_1	m_2	m_3	...
u_1				
u_2				
u_3				
...				

We fill in each cell (u_k, m_i) in accordance with the following symbols:

"≡" means that u_k is a multiple of m_i, or, in other words, that $x^k + y^k \equiv z^k \bmod m_i$;

"~≡" means that u_k is a *not* a multiple of m_i, or, in other words, that $x^k + y^k$ is *not* $\equiv z^k \bmod m_i$;

"|||*c*" means that $<x^k + y^k,\ z^k>$ is congruent to the *c*ounterexample element $<x^p + y^p,\ z^p>$ mod m_i, or, in other words, that $<x^k + y^k,\ z^k>$ and $<x^p + y^p,\ z^p>$ are in the same **C**-set mod m_i;
"|||~c" means that $<x^k + y^k,\ z^k>$ is *not* congruent to $<x^p + y^p,\ z^p>$ mod m_i, or, in other words, that $<x^k + y^k,\ z^k>$ and $<x^p + y^p,\ z^p>$ are *not* in the same **C**-set mod m_i;

Each cell thus has one of the following pairs of symbols:

"≡" , "|||*c*", or
"≡" , |||~*c*, or
~≡ , |||~*c*.
(We use "|||" because it suggests the "vertical congruence" imposed by Fermat's Little Theorem.)

No cell can contain the pair <~≡ , |||*c*>, because that would mean that $<x^p + y^p,\ z^p>$ is in a non-congruent **C**-set, which is impossible. We also point out that, with one exception, each row (each u_k) can have only a finite number of pairs whose first term is "≡" because there are only a finite number of factors in u_k, hence only a finite number of m_i such that $u_k = nm_i$, the condition for congruence. The one exception is u_p, which by assumption of a counterexample equals 0. Thus $x^p + y^p \equiv z^p \mod m_i$ for all i and therefore each cell in the u_p row contains <≡ , |||*c*>.

The question is, can we derive a contradiction from these relationships? In trying to answer this question, we must remember that each **C**-set contains an infinity of elements. Thus, the contents of each cell, regardless which of the above three pairs of symbols the cell contains, must be duplicated in an infinity of cells in the same column (same m_i). In particular:

For each m_i, a countable infinity of cells must contain the pair <"≡" , "|||*c*">. The reason is that, for each m_i, there is a (congruent) **C**-set containing the element $<x^p + y^p, z^p>$, and since a **C**-set contains an infinity of elements, an infinity of cells must contain <"≡" , "|||*c*">.

We also remind the reader of the facts concerning an infinite succession of prime moduli, q, q^2, q^3, ..., as discussed under ""Consequences" of a Counterexample" on page 11.

In passing, we mention the following possible tactic: begin with the assumption that no counterexamples exist, and then show that there is no way, in the above table, to change the contents of the requisite cells to <"≡" , "|||*c*"> as required by a counterexample. Would that give us a proof of FLT?

Approach Type VI: Show that the Assumption of a Counterexample Implies a Contradiction in the $U_{\_k}$

First Implementation

Let $U_k = x^k + y^k - z^k$, where $k \geq 1$. "Lemma 60.0:" on page 12 states that if a counterexample exists, then for each modulus q^j, where q is a prime and $j \geq 1$, there are a finite number of residue classes mod q^j that contain no U_k, and furthermore among those residue classes that *do* contain U_k's, there is always one congruent to 0, that is, there is always the unique residue class mod q^j that contains all multiples of q^j.

If we can show that this consequence of the existence of a counterexample is impossible, then we have a proof of FLT.

Second Implementation

Let q be *any* prime and consider a modified **C**-set mod q containing the counterexample element $< x^p + y^p, z^p >$. The modification is that we ignore the base element, and instead merely consider the infinity of elements $< x^k + y^k, z^k >$, where $k \equiv p \bmod q - 1$, and $k > p$. Then by definition of congruence, we have:

$x^k \equiv x^p \bmod q$,
$y^k \equiv y^p \bmod q$, and
$z^k \equiv z^p \bmod q$,

which in turn implies that there exist non-zero u, v, w, such that

$x^k - qu = x^p$,
$y^k - qv = y^p$, *and*
$z^k - qw = z^p$.

Thus, from $x^k + y^k - z^k = U_k$; we have

$(x^p + qu) + (y^p + qv) - (z^p + qw) = U_k$.

Assumption of a counterexample yields

$qu + qv - qw = U_k$, or $q(u + v - w) = U_k$.

What we have just established applies to *all primes q* and to *all k such that* $k \equiv p$ *mod* $q - 1$. Furthermore, similar facts apply to *all* ***C****-sets mod* q^r, where $r \geq 1$, which contain the counterexample element $< x^p + y^p, z^p >$. Furthermore, similar facts apply to *all* ***C****-sets mod m*, where m is a composite number that is relatively prime to at least two of *x, y, z.* (There is an infinity of such composites, because there is an infinity of primes but only a finite number of different primes in *x, y,* and *z.*) In the case of composite moduli, we must use Euler's generalization of Fermat's Little Theorem (see "Fermat's Little Theorem" on page 7).

If we can find a contradiction in the set of facts concerning the U_k's we will have a proof of FLT. However, initial attempts have not been promising, not even when we consider a modulus m as described in the previous paragraph, an m containing powers of, say, n different primes, and then investigate the exponent $p + j\varphi(m)$ of x, y, z in the modulus m, and in the modulus of each of the different primes.

A related Approach is to show that there exists an appropriate modulus m such that for each k, where $1 \leq k \leq \varphi(m) - 1$, $(U_k, m) = 1$. If such a modulus exists, then $< x^p + y^p, z^p >$ is an element of a non-congruent **C**-set mod m, which is a contradiction, and gives us a proof of FLT.

We can relax the condition on U_k and still achieve a contradiction and a proof of FLT if we can show that $< x^p + y^p, z^p >$ is an element of a non-congruent **C**-set, that is, a **C**-set such that U_k for its base element is relatively prime to m.

For details, see “Lemma 60.0”, “An Approach Via Congruence of Exponents”, and other sections containing “U_k” in Part (4) of this paper.