

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@cs.com

Phone: (510) 548-3827

Apr. 25, 2011

Key words: Fermat's Last Theorem

Definition of “Line-and-Circles” Model of Congruence

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

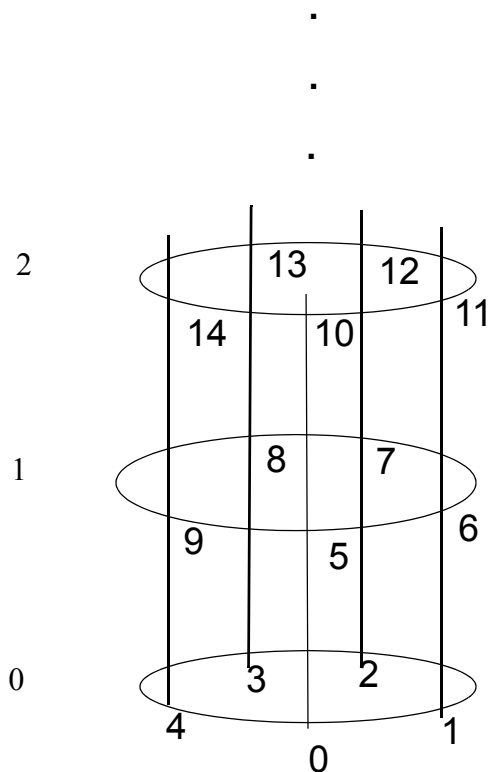


Fig. 1. “Geometrical” model of positive integers congruent mod 5.

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

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

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

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

concerned with ordered pairs, $\langle x^k + y^k, z^k \rangle$.

(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 \underline{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 $a \equiv a^p \pmod{p}$. 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 $a \equiv a^{\varphi(m)+1} \pmod{m}$ 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, we will use the term *appropriate modulus* to mean either (1) any prime modulus q , since in this case it doesn’t matter if one of x, y, z has a factor q or (2) a composite modulus m such that $(x, m) = (y, m) = (z, m) = 1$.

Definition of “Congruent Ordered Triples”

Let $\langle u, v, w \rangle, \langle u', v', w' \rangle$ be ordered triples, where u, v, w, u', v', w' are positive integers. Then if, for some modulus m , $u \equiv u', v \equiv v',$ and $w \equiv w' \pmod{m}$, we say that the *ordered triples are congruent mod m* and that $\langle u, v, w \rangle$ is congruent to $\langle u', v', w' \rangle \pmod{m}$. We will omit *mod m* when m is understood. For a triple $\langle u, v, w \rangle$ there are two possibilities: $u + v \equiv w \pmod{m}$, or $u + v \not\equiv w \pmod{m}$. 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. If, in a set of congruent ordered triples, there is no triple below a triple t , then we say that t is the *bottom triple* of the set.

Definition of “ $U(k, a, b, c)$ ”

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

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 (we assume) $x + y \not\equiv z \pmod{p}$.

But then, by Fermat’s Little Theorem, $x^p + y^p \not\equiv z^p \pmod{p}$, 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 is at least one error in this argument, namely, that $x + y \not\equiv z \pmod{p}$. But there are only two ways for $x + y > z$ to imply that $x + y \not\equiv z \pmod{p}$. One is for $x + y$ and z to be less than p . But this is impossible, since, by part (a) of Lemma 1.0 in Part (1), 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.occampress.com). This strategy is called, informally, the “pushing-up” or “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 i -level counterexample tuples in each i -level tuple-set, 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 idea underlying 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, $\langle x^p + y^p, z^p \rangle$, 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 $\langle u^j + v^j, w^j \rangle$, 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 $\langle u^j + v^j, w^j \rangle$ there are two possibilities. For all $i \geq 0$:

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

If (1) holds, then we try to show that for all i , $u^{j+i\phi(m)} + v^{j+i\phi(m)}$ and $w^{j+i\phi(m)}$ 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 $\langle u^{j+i\phi(m)} + v^{j+i\phi(m)}, w^{j+i\phi(m)} \rangle$ 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)

After a great deal of effort, we have been unable to make this strategy work, although it is discussed at length in the section, “Approaches Via C-Sets” on page 9.

Approaches Via D-Sets

Definition of D-set

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

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

Each **D**-set constitutes elements of a congruence class mod q , and there is always an infinity of elements in each **D**-set, since there is always an infinity of $r \equiv j \pmod{q-1}$ for each j .

We now state the following facts. Each fact is indicated by a letter in parentheses.

(A) For each q , the total number of **D**-sets is $q^3(q-1)$, since there are q^3 possible ordered triples $\langle u, v, w \rangle$ and for each such ordered triple there are $(q-1)$ possible exponents j .

(B) In each **D**-set mod q , all $U(r, a, b, c)$ are congruent mod q . (Because $a^r \equiv u^j, b^r \equiv v^j, c^r \equiv w^j \pmod{q}$ and $U(r, a, b, c) = a^r + b^r - c^r$.)

(C) There exist r, a, b, c such that $U(r, a, b, c)$ is negative. For example, if $a < b < c$ (as must be the case for a counterexample), then for all sufficiently large r , $U(r, a, b, c)$ is negative.

(D) For each ordered triple $\langle a, b, c \rangle$ there exists a minimum modulus q such that for all prime moduli $q' \geq q$, $a = u$, $b = v$, and $c = w$, where u, v, w are the minimum residues in the definition of a **D**-set. This, of course, applies to the ordered triple $\langle x, y, z \rangle$, where x, y, z are the constituents of a counterexample if a counterexample exists.

(E) For each ordered triple $\langle a, b, c \rangle$, and for each prime modulus q :

$a \equiv u \pmod{q}$ for some minimum residue u ,
 $b \equiv v \pmod{q}$ for some minimum residue v ,
 $c \equiv w \pmod{q}$ for some minimum residue w ,

hence $U(1, a, b, c) \equiv U(1, u, v, w) \pmod{q}$;

and therefore

$a^2 \equiv u^2 \pmod{q}$,
 $b^2 \equiv v^2 \pmod{q}$,
 $c^2 \equiv w^2 \pmod{q}$,

hence $U(2, a, b, c) \equiv U(2, u, v, w) \pmod{q}$;

...

$$\begin{aligned} a^{q-1} &\equiv u^{q-1} \pmod{q}, \\ b^{q-1} &\equiv v^{q-1} \pmod{q}, \\ c^{q-1} &\equiv w^{q-1} \pmod{q}, \end{aligned}$$

hence $U(q-1, a, b, c) \equiv U(q-1, u, v, w) \pmod{q}$.

(F) For each prime modulus q , and for each $U(r, a, b, c)$ (including $U(p, x, y, z)$), $U(r, a, b, c)$ is an element of a congruence class mod q . (*Proof:* follows from definition of **D**-set, and in particular from the fact that in each $U(r, a, b, c)$, r is congruent to some j in $\{1, 2, 3, \dots, j-1\}$ by Fermat's Little Theorem.)

For a only a finite number of prime moduli q , each $U(r, a, b, c)$ (excluding $U(p, x, y, z)$) is an element of a congruence class mod q that is congruent to $0 \pmod{q}$. Hence $U(r, a, b, c)$ is a multiple of q . (*Proof:* there are only a finite number of prime factors q in each $U(r, a, b, c)$. For each such q , $U(r, a, b, c)$ is congruent to $0 \pmod{q}$, hence is a multiple of q .)

Let $S = \{U(r, a, b, c)\}$. If a counterexample exists, then each prime q is a factor of an infinity of elements of S . If a counterexample does not exist, this is not necessarily true. (*Proof:* If a counterexample exists, then for all prime moduli q , $U(p, x, y, z) = 0$ and the congruence class containing 0 (like all congruence classes) has an infinity of elements. If a counterexample does not exist, then it is not necessarily true that for each prime modulus q , there exists a $U(r, a, b, c)$ (hence an infinity of $U(r', a, b, c)$) such that $U(r, a, b, c)$ has the prime factor q .)

The fact that if a counterexample exists, then each prime q is a factor of an infinity of elements of S , whereas this is not necessarily true if a counterexample does not exist, is an example of the “consequences” of the existence of a counterexample. For a further discussion, see ““Consequences” of a Counterexample” on page 14.

Approaches via D-sets

The most promising approach, in our opinion, is to find a contradiction by comparing the two cases, a counterexample exists and a counterexample does not exist, using the terms $U(r, a, b, c)$. The reader is encouraged to refer to “Appendix B — Approach Via the Fixed Set” on page 32. We here point out that since, prior to Wiles’ proof of FLT it was known that the exponent p in any counterexample must be greater than 125,000, and that $p < x$, clearly, for *many* prime moduli q , all minimum elements u^j , v^j and w^j in **D**-sets mod q are less than x^p , y^p and z^p respectively. Thus these u^j , v^j and w^j will be the same regardless if a counterexample exists or not, for the reason set forth in Appendix B. This fact may enable us to arrive at a contradiction involving the U terms.

We must add that, for a long time, we believed it might be possible to develop a proof by contradiction from the fact¹ that:

$$\begin{aligned} x^{p-(q-1)} + y^{p-(q-1)} - z^{p-(q-1)} &= U((p-(q-1)), x, y, z) \geq 0 \\ x^{p-2(q-1)} + y^{p-2(q-1)} - z^{p-2(q-1)} &= U((p-2(q-1)), x, y, z) \geq 0 \\ x^{p-3(q-1)} + y^{p-3(q-1)} - z^{p-3(q-1)} &= U((p-3(q-1)), x, y, z) \geq 0 \\ \dots \\ x^{p-s(q-1)} + y^{p-s(q-1)} - z^{p-s(q-1)} &= U((p-s(q-1)), x, y, z) \geq 0, \end{aligned}$$

1. See part (a) of Lemma 1.5 in Part (1) of this paper (www.occampress.com) for a proof that each of these U terms ≥ 0 .

where q is small enough such that s , the quotient of p divided by q , is a positive integer. Our hope was that we might be able to show that

$$x^{p-s(q-1)} + y^{p-s(q-1)} - z^{p-s(q-1)} = U((p-s(q-1)), x, y, z) = 0,$$

implying that there was a minimum counterexample smaller than our minimum counterexample $x^p + y^p - z^p$, a contradiction that would give us a proof of FLT.

But in fact for *any* a, b, c such that $a < b < c < r$, the same sequence of equations, beginning with $a^r + b^r - c^r = U(r, a, b, c)$ holds for the appropriate q . So this strategy seems unpromising.

At present we believe that fact (F) above is worth investigating with the aim of showing that there are “too many” prime factors q in the elements of the set $\{U(r, x, y, z)\}$.

We remind the reader who has read “Appendix B — Approach Via the Fixed Set” on page 32 that for all k , where $1 \leq k \leq s$,

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

is in the fixed-set F , meaning that these $U((p-k(q-1)), x, y, z)$ are the same whether or not a counterexample exists.

Approaches Via C-Sets

C-sets are an earlier version of **D**-sets.

Summary of Approaches

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 $a \equiv x, b \equiv y, c \equiv z \pmod{m}$.

(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 $\langle x^p + y^p, z^p \rangle$ is an element of a non-congruent **C**-set (definition given below). (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 $\langle x^p + y^p, z^p \rangle$.

(Type VI) Show that the assumption of a counterexample implies a contradiction in the $U(k, a, b, c)$, where $U(k, a, b, c) = a^k + b^k - c^k$.

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 $m, a + b \equiv c \pmod{m}$.

Informally: "Equality implies congruence".

(2) If $a + b \neq c$, then

(a) for an infinite number of moduli $m, a + b \not\equiv c \pmod{m}$;

(b) for a finite number of moduli, it is possible that $a + b \not\equiv c \pmod{m}$ or $a + b \equiv c \pmod{m}$.

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, $a + b \not\equiv c \pmod{m}$.

Proof of (b):

If r is as defined in “Proof of (a)”, and r is a multiple of the modulus m , then $a + b \equiv c \pmod{m}$ by definition of congruence; otherwise $a + b \not\equiv c \pmod{m}$. \square

Example:

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

(3)

If $a + b \equiv c \pmod{m}$, 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 $a + b \not\equiv c \pmod{m}$, 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 $a^q \equiv a \pmod{q}$. Euler’s generalization states: if $(a, m) = 1$ then $a^{\varphi(m)} \equiv 1 \pmod{m}$, where m is prime or composite, and φ is Euler’s totient function¹. For a prime q , $\varphi(q) = q - 1$.

Fermat’s Little Theorem implies $a^q \equiv a \pmod{q}$, $a^{q+1} \equiv a^2 \pmod{q}$, $a^{q+2} \equiv a^3 \pmod{q}$, ..., $a^{2q-2} \equiv a^{q-1} \pmod{q}$, etc. In other words, Fermat’s Little Theorem implies that for $1 \leq j \leq q - 1$, $a^j \equiv a^{j+k(q-1)} \pmod{q}$, where $k \geq 0$. Thus, for example, if $q = 5$, then $3^1 \equiv 3^5 \pmod{5}$; $3^2 \equiv 3^6 \pmod{5}$, 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 $a \equiv b \pmod{m}$, then whatever is true modular-arithmetically of a is true modular-arithmetically of b . In particular, if $(a, m) = (b, m) = 1$, then if $a^r \equiv b \pmod{m}$, where $r \geq 1$, and $a \equiv c \pmod{m}$, then $c^r \equiv b \pmod{m}$. In particular, we have:

(1.91) (c)

If $(a, m) = (b, m) = (c, m) = 1$, and if

$a \equiv a' \pmod{m}$, and $b \equiv b' \pmod{m}$, and $c \equiv c' \pmod{m}$, then

if $a^r + b^r \equiv c^r \pmod{m}$, $r \geq 1$,

then $a^{r'} + b^{r'} \equiv c^{r'} \pmod{m}$ and

$a^r \equiv a^{r'} \pmod{m}$ and $b^r \equiv b^{r'} \pmod{m}$ and $c^r \equiv c^{r'} \pmod{m}$.

(See “(1.91) (c)” on page 6 of Part (2) of this paper, on the web site occampress.com.)

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

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 10. Suppose that q is a prime such that $(x, q) = (y, q) = (z, q) = 1$, and suppose that $p \equiv j \pmod{q-1}$, 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 in the section “Moduli” on page 11.) Then by Fermat’s Little Theorem:

$$\begin{aligned} x^p + y^p &\equiv z^p \pmod{q} \text{ (non-congruence would imply inequality) and also} \\ x^{p-(q-1)} + y^{p-(q-1)} &\equiv z^{p-(q-1)} \pmod{q} \text{ and} \\ x^{p-2(q-1)} + y^{p-2(q-1)} &\equiv z^{p-2(q-1)} \pmod{q} \text{ and} \\ &\dots \\ x^j + y^j &\equiv z^j \pmod{q}, \text{ where } 1 \leq j \leq q-1. \end{aligned}$$

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 proof of FLT, because if $x^j + y^j \neq z^j$ then we have a contradiction, since that inequality implies non-congruence for the counterexample. 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 $q^1, q^2, q^3, \dots, q^k, \dots$, where q^k is the first modulus such that $x^p + y^p$ 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 10. 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 that is reduced. Assume that $x^p + y^p \equiv z^p \pmod{q}$ (non-congruence would imply inequality). Then for all a', b', c' such that $a' \equiv x, b' \equiv y$, and $c' \equiv z \pmod{q}$, and $a' \leq x$, and $b' \leq y$, and $c' \leq z$, where at least one “ \leq ” is “ $<$ ”, we have, by (1.91)(c) that $a'^p + b'^p \equiv c'^p \pmod{q}$.

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 if $a'^p + b'^p \neq c'^p$ then we have a contradiction, since inequality implies non-congruence for the counterexample. On the other hand if $a'^p + b'^p = c'^p$ then we also have a contradiction, namely, a smaller counterexample (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 condition 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, $q^1, q^2, q^3, \dots, q^k, \dots$, 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 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 x, y, z . Furthermore, Lemma 1.0 in Part (1) 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 counterexample. 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 $q < x$.

A proof that a q exists that is less than y , or less than x , is given in “Lemma 30.0: Statement and Proof” on page 18 of Part (2) of this paper, on the web site occampress.com.

Another reason why we were wrong in believing that there might not be a prime q that is less than y , or less than x is that, by Lemma 1.0 in Part (1) of this paper, $p < x < y < z$. Taking p as modulus is discussed above in “Supporting Material for Approaches I - VI” on page 9 and in Appendix C of Part (1).

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 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 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 $x^k + y^k \not\equiv z^k \pmod{m}$. 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 $x^k + y^k \not\equiv z^k \pmod{m}$.

Trade-offs in the Size of Moduli

It is important that we keep in mind a fundamental trade-off in the size of moduli: 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 , $a^r + b^r \not\equiv c^r \pmod{m}$. If $a^r \equiv x^p$, $b^r \equiv y^p$, and $c^r \equiv z^p \pmod{m}$, then we have a contradiction and a proof of FLT.

On the other hand, the smaller the modulus, the greater the number of a, b, c congruent to x, y, z and less than x, y, z . Also, a small modulus m increases the chances that $m < p < x < y < z$, which is of advantage in several Approaches.

Definition of C-set

We want to capture, for each modulus m such that $(x, m) = (y, m) = (z, m) = 1$, certain ordered pairs $\langle a^r + b^r, c^r \rangle$, 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 10 and "(1.91) (c)" on page 10. For a modulus $m \geq 2$, we define a C-set $C_{u, v, w, j, m} \pmod{m}$ as follows:

$$C_{u, v, w, j, m} = \{ \langle u^r + v^r, w^r \rangle \mid r \equiv j \pmod{\varphi(m)}, u^r, v^r, w^r \text{ are each less than } m, \text{ and } m \text{ is an appropriate modulus} \}.$$

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

By definition of congruence, each $C_{u, v, w, j, m}$ also contains all $\langle a^r + b^r, c^r \rangle$ 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 $\langle u^r + v^r, w^r \rangle$ in a C-set we call an *element* of the C-set. The ordered pair $\langle u^j + v^j, w^j \rangle$ we call the *base element* of the C-set. If a counterexample $x^p + y^p = z^p$ exists, we call the element $\langle x^p + y^p, z^p \rangle$ the *counterexample element*. It is immediately clear that the counterexample 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 $\langle x^p + y^p, z^p \rangle$ is then an element of a non-congruent C-set, a contradiction.

It is clear that for each modulus m , the counterexample element $\langle x^p + y^p, z^p \rangle$ 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 $m = 2, 3, 4, \dots$. As m increases, each $\langle c^p + d^p, e^p \rangle$ 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 $\langle c^p + d^p, e^p \rangle$ as base element is necessarily non-congruent because $c^p + d^p \neq e^p$. Yet it must be the case that the element $\langle x^p + y^p, z^p \rangle$ is never in a non-congruent C-set. So it must be that for all elements $\langle c^p + d^p, e^p \rangle$ that are base elements of C-sets containing $\langle x^p + y^p, z^p \rangle$, $c^p + d^p$ and e^p cannot each be less than m , and, furthermore, it must be the case that $\langle c^p + d^p \equiv e^p \rangle$, since the element $\langle x^p + y^p, z^p \rangle$ must always be in a congruent C-set and, furthermore the element $\langle x^p + y^p, z^p \rangle$ must always equal an element $\langle u^r + v^r, w^r \rangle$ in a congruent C-set, and, furthermore, at some m , the ele-

ment $\langle x^p + y^p, z^p \rangle$ 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 $\equiv z^k \pmod m$ for all m (an infinite number) such that r_k is not a multiple of m , regardless whether $\langle x^k + y^k, z^k \rangle$ 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 $\equiv z^k \pmod m$ (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:

$$\begin{aligned} r_k &\text{ is not a multiple of } m; \\ x^k &\equiv x^p, y^k \equiv y^p, z^k \equiv z^p \pmod m; \\ (x, m) &= (y, m) = (z, m) = 1. \end{aligned}$$

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 $\langle x^p + y^p, z^p \rangle$, because that would be a contradiction.

“Consequences” of a Counterexample

Readers who first contemplate the infinite sequence of cases,

$$\begin{aligned} x^1 + y^1 &\neq z^1, \\ x^2 + y^2 &\neq z^2, \\ x^3 + y^3 &\neq z^3, \\ x^4 + y^4 &\neq z^4, \\ &\dots \\ x^{p-1} + y^{p-1} &\neq z^{p-1}, \\ x^p + y^p &= z^p, \\ x^{p+1} + y^{p+1} &\neq z^{p+1}, \\ &\dots \end{aligned}$$

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 $\langle x^p + y^p, z^p \rangle$ touches down at q^k (as it must, for some $k \geq 1$), then for all $k + j, j \geq 1$, $x^p + y^p \equiv z^p \pmod{q^{k+j}}$. 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 “Definition of ‘Line-and-Circles’ Model of Congruence” on page 2)), then since $x^p + y^p = z^p$, $x^p + y^p \equiv z^p \pmod{q^{k+j}}$. It follows that for all moduli q^{k+j} , $\langle x^p + y^p, z^p \rangle$ 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 $\langle a^r + b^r, c^r \rangle$. 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.

Let q be a prime. Let $S_k = \{ \langle a^r, b^r, c^r \rangle \mid a^r \equiv x^k, b^r \equiv y^k, c^r \equiv z^k \pmod{q} \}$. We say that each triple $\langle a^r, b^r, c^r \rangle$ is congruent to the triple $\langle x^k, y^k, z^k \rangle$. We observe that there are two ways that a triple $\langle a^r, b^r, c^r \rangle$ can be an element of S_k .

One is via Fermat’s Little Theorem (which states that if p is prime, then $a \equiv a^p \pmod{p}$). This implies that if

$$r \equiv k \pmod{q-1},$$

then $x^r \equiv x^k, y^r \equiv y^k, z^r \equiv z^k \pmod{q}$.

The other is via “(1.91) (c)” on page 10, which implies that if

$$a \equiv x \pmod{q}, \text{ and } b \equiv y \pmod{q}, \text{ and } c \equiv z \pmod{q}, \text{ and if}$$

$$x^r + y^r \equiv z^r \pmod{q}, \text{ then}$$

$$a^r + b^r \equiv c^r \pmod{q}.$$

For all $k \geq 1$, and for all positive integers k, a, b, c , such that $\langle a^r, b^r, c^r \rangle$ is congruent to the triple $\langle x^k, y^k, z^k \rangle$, let $U(k, a, b, c) = a^k + b^k - c^k$. (Note that k, a, b, c can equal p, x, y, z , respectively.)

Then:

(a) the $U(k, a, b, c)$ are partitioned into $q - 1$ sets, each set a proper subset of a residue class mod q . The $U(k, a, b, c)$ in exactly one of these sets, namely, the set containing $U(p, x, y, z)$, are all multiples of q .

(b) (This part has been removed because it was not correct.)

(c) Each $U(k, a, b, c)$ is a multiple of 2.

(d) For each prime q , if $U(k, a, b, c)$ is a multiple of q , then at least one of a^k, b^k, c^k must be greater than q .

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

Parts of Lemma 60.0 are exploited in “Approach Type VII: Show that the assumption of a

counterexample implies a contradiction in the U(k, a, b, c)” on page 27.

Further examples of the consequences of a counterexample are shown in the following.

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 $\langle nx^p + ny^p, nz^p \rangle$ 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 $\langle a^r + b^r, c^r \rangle$. *None of these elements would be congruent if the counterexample did not exist.* So the existence of the counterexample has more “consequences”.

Furthermore, since $a^r + b^r \equiv c^r \pmod{q^{k+j}}$ implies (by definition of congruence) that there exists a U such that $a^r + b^r + Uq^{k+j} = c^r$, 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 $a^r + b^r \equiv c^r \pmod{q^i}$. 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 $\langle a^r + b^r, c^r \rangle$.

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.* For further details, see “First Implementation” on page 17, that is, First Implementation of Approach Type I.

Two attempts to apply the fact that a counterexample has consequences to a proof of FLT will be found in “Approach Type VII: Show that the assumption of a counterexample implies a contradiction in the U(k, a, b, c)” on page 27, and in part (E) of “Approach Type IV: Considering All Multiples of All Powers of a, b, c” on page 27.

Approach Type I

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, $10 + 2 = 12$ ($d = 10, e = 2, f = 12$; $j = 2, k = 1, l = 3$).

Implementations of Approach Briefly Described

In Approach Type I, we try to show that the triples $\langle x^p, y^p, z^p \rangle$ and $\langle a^k, b^k, c^k \rangle$ give rise to a contradiction. We attempt to do this via several implementations:

First Implementation: show that a contradiction arises between $\langle a^k, b^k, c^k \rangle$ that are congruences but *are not* equalities, and $\langle a^k, b^k, c^k \rangle$ that are congruences *and are* equalities.

Second Implementation: show, via an equation, that a congruence that is *not* an equality is equal to a congruence that *is* an equality, an obvious contradiction.

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

Fourth Implementation: show that a contradiction arises if we consider all $\langle a^p, b^p, c^p \rangle$ that

have touched 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 . This quotient is a level number in our lines-and-circles model of congruence.)

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 and Equalities

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:

$|T| = s(z^p - q) + s(z^p - 2q) + \dots + s(z^p - tq)$, where tq is the largest multiple 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 $\langle a^p, b^p, c^p \rangle$.

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

If we can show that the assumption of a counterexample implies that there exist h, i, j, m, n, r such that

$$(x^p - hq) + (y^p - iq) - (z^p - jq) = (x - mq)^p + (y - nq)^p - (z - rq)^p, \text{ where } h + i = j.$$

then we will have a contradiction, for the left-hand side must equal 0, since it is derived from an equality that is in turn derived from the counterexample equality, and the right-hand side is derived from a p -exponent triple, and by Lemma 60.0 we know that therefore the right-hand side cannot equal 0.

Third Implementation

This Implementation is being revised.

Fourth Implementation

Let Q denote a finite sequence of successive prime moduli $2, 3, 5, 7, \dots, q_i, \dots, q_n$ such that the assumed minimum counterexample $x^p + y^p = z^p$ touches down at the last modulus in the sequence (q_n). For each modulus q in the sequence, let

T_q denote the set $\{ \langle a^p, b^p, c^p \rangle \mid a^p + b^p \text{ and } c^p \text{ are each less than } q \}$.

V_q denote the set $\{ \langle a^p, b^p, c^p \rangle \mid a^p \equiv x^p, b^p \equiv y^p, c^p \equiv z^p \pmod{q} \}$.

Part (d) of “Lemma 60.0:” on page 15 implies that no element of T_q can be an element of V_q . And yet every possible a, b, c , up to the limit imposed by the size of q , is present in the $\langle a^p, b^p, c^p \rangle$ in T_q as the sequence of q progresses. Thus, initially we have $\langle 1^p, 1^p, 1^p \rangle$ in T_3 .

If we can show that the fact that no element of T_q can be an element of V_q implies a contradiction, we will have a proof of FLT.

Fifth Implementation

Note: This is an earlier version of “First Implementation” on page 17.

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 counterexample. 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 $x^p \pmod{m}$; 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 $\{x^n + y^n \equiv z^n \pmod{m} \mid n = p - j \cdot \varphi(m), j \geq 1, \text{ and } n \text{ is positive}\}$. That these are congruences follows from “Fermat’s Little Theorem” on page 10. That each congruence is an inequality follows from “Definition of ‘Minimum Counterexample’” in Part (1). 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 $\{a^p + b^p \equiv c^p \pmod m \mid a, b, c \text{ are less than } x, y, z \text{ respectively and } a \equiv x, b \equiv y, \text{ and } c \equiv z \pmod m\}$. That these are congruences follows from “(1.91) (c)” on page 10. That each congruence is an inequality follows from “Definition of ‘Minimum Counterexample’” in Part (1). 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 $\langle u, v, w \rangle$ such that $u < x^p, v < y^p$, and $w < z^p$ and $u \equiv x^p, v \equiv y^p$, and $u \equiv z^p \pmod m$;
- 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 inequalities 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 14). 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 $\leq z$. 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 11. The reader is encouraged to read that section before reading the rest of this section.]

Now part (a) of Lemma 1.0 in Part (1) 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 $\phi(q)$, there exists one C-set whose base element is $\langle u^p + v^p, w^p \rangle$. The reason is that $p < x < q$ implies $p < \phi(q) = q - 1$. 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 $\langle u^p + v^p, w^p \rangle$, 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 $z \equiv w \pmod q$, where $w < q$ and we have

$x^p + y^p \equiv w^p \pmod{q}$ (by “(1.91) (c)” on page 6 of Part (2) of this paper, on the web site occam-press.com). Since by assumption $x^p + y^p = z^p$, we also have $x^p + y^p \equiv z^p \pmod{q}$. 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, \dots

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 $\langle x^p + y^p, z^p \rangle$ is *always* the base element of each **C**-set mod q^k , where $k \geq 1$, in which it is an element. The reason is that since, as is well-known, $\phi(q^k) = (q - 1)q^{k-1}$, it follows that $p - \phi(q^k)$ is negative. Thus, if $n = p - j(\phi(q^k))$, where $j \geq 1$, there cannot be an element $\langle x^n + y^n, z^n \rangle$ in a **C**-set mod q^k . Thus our hope of proving that $\langle x^p + y^p, z^p \rangle$ 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 $\langle x + y, z \rangle$ is the base element of a **C**-set. In the set of **C**-sets mod q^2 such that the base elements are $\langle x^j + y^j, z^j \rangle$, where $1 \leq j \leq \phi(q^2)$, there exists one **C**-set whose base element is $\langle x^p + y^p, z^p \rangle$, since if $p < x < q$ then $p < \phi(q^2) = q(q - 1)$.

The **C**-set whose base element is $\langle x^p + y^p, z^p \rangle$ 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 $a^r + b^r \equiv c^r \pmod{q^2}$, where $a \equiv x, b \equiv y, c \equiv z \pmod{q^2}$, and $r \equiv p \pmod{\phi(q^2)}$. (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 14.)

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 $k \geq 1$. 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 $\equiv c^r \pmod{q^k}$, 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 $a^r + b^r \equiv c^r \pmod{q^k}$ 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 $1a, 2a, 3a, \dots, ma$, contains the set of all residue classes mod m in some order. If the sequence continues — $(m + 1)a, (m + 2)a, \dots, 2m(a)$ — 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 19 and let $k \geq 1$. Then $\langle x^p + y^p, z^p \rangle$ is an element (not necessarily the base element) of a congruent **C**-set mod q^k . Now consider the sequence of elements,

$$(1) \\ \langle 1x^p + 1y^p, 1z^p \rangle \\ \langle 2x^p + 2y^p, 2z^p \rangle$$

$$\langle 3x^p + 3y^p, 3z^p \rangle$$

$$\dots$$

$$\langle q^k x^p + q^k y^p, q^k z^p \rangle.$$

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 $\langle nx^p + ny^p, nz^p \rangle$ 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 $\langle x^j + y^j, z^j \rangle$, where $j \geq 1$, $j \neq p$, and $x^j + y^j$ and z^j are each less than q^k . In these cases, the base element $\langle x^j + y^j, z^j \rangle$ 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 $\equiv z^j \pmod{q^k}$. 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 utilize the known non-congruent C-sets. These *include* the ones having base element $\langle u^j + v^j, w^j \rangle$, where $1 \leq j \leq \varphi(q^k)$, and where $u^j + v^j$ is not $\equiv w^j \pmod{q^k}$. 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 $\langle x^j + y^j, z^j \rangle$, 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 $\equiv z^j \pmod{q^k}$ — 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 $\langle x^p + y^p, z^p \rangle$.

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 $\langle x^p + y^p, z^p \rangle$ 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 $a^p + b^p \equiv c^p \pmod{q}$ 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 $a^p + b^p \equiv c^p \pmod{q}$ 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 $a^p + b^p \equiv c^p \pmod{q}$ 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 $\langle 16 + 17, 33 \rangle$. It is true that $16 + 17 = 33$, and therefore that $16 + 17 \equiv 33 \pmod{7}$. It is also true that $16 \equiv 9 \pmod{7}$, $17 \equiv 10 \pmod{7}$, $33 \equiv 19 \pmod{7}$, $9 + 10 \equiv 19 \pmod{7}$, 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 $x^p + y^p \equiv z^p \pmod{q}$ 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 $c \equiv z \pmod{q}$, and
 $a^p + b^p \equiv c^p \pmod{q}$ 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

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

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 $\langle u^k + v^k, w^k \rangle$, where $1 \leq k \leq \varphi(m)$. 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 $1 \leq k \leq \varphi(m)$, the **C**-set containing $\langle x^k + y^k, z^k \rangle$ is non-congruent. For the counterexample element $\langle x^p + y^p, z^p \rangle$ 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 $\langle x^p + y^p, z^p \rangle$ 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 $p \leq \varphi(m)$. 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 $\phi(m_{max})$ is less than 125,000. Then FLT is true for all x, y, z such that $(x, m) = (y, m) = (z, m) = 1$, where $m \leq m_{max}$, 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, $q, q^2, q^3, q^4, \dots, q^k, \dots$. 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 $\langle a^r + b^r, c^r \rangle$ 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 $\langle x^p + y^p, z^p \rangle$. 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 $1 \leq k < \phi(q) = q - 1$ it is the case that
 $k \equiv p \pmod{q - 1}$ and
 $x^k \equiv x^p \pmod{q}$,
 $y^k \equiv y^p \pmod{q}$,
 $z^k \equiv z^p \pmod{q}$, and
 $(U_k, q) = 1$, implying that $x^k + y^k \not\equiv z^k \pmod{q}$,
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 $n \equiv k \pmod{q - 1}$ (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, $x^k + y^k \not\equiv z^k \pmod{q}$, 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 $j \equiv h \pmod{q-1}$, then for each u, v , $u^j \equiv v^h \pmod{q}$, and so we can eliminate the explicit listing of the conditions $x^k \equiv x^p \pmod{q}$, $y^k \equiv y^p \pmod{q}$, and $z^k \equiv z^p \pmod{q}$. 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
 $k \equiv p \pmod{q-1}$ and
 $(U_k, q) = 1$, implying that $x^k + y^k \not\equiv z^k \pmod{q}$,
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 in Part (1), 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 ‘Smaller Prime’ Lemma” in Part (1).

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 $x^k + y^k \not\equiv z^k \pmod{q}$.

Then FLT is true.

The proof is the same as that given under “Conditions for the Truth of FLT” on page 23. 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 10 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” in Part (1) 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 in Part (1), each U_k is a multiple of p , which is in our favor, since by “The ‘Smaller Prime’ Lemma”, 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 $(U_1, q) = (U_2, q) = \dots = (U_{q-1}, q) = 1$. 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 “Definition of C-set” on page 13, that $x^p + y^p \not\equiv z^p \pmod{q}$, 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

$$\begin{aligned} x^k &\equiv x^p \pmod{q}, \\ y^k &\equiv y^p \pmod{q}, \text{ and} \\ z^k &\equiv z^p \pmod{q}, \end{aligned}$$

then it follows, by what we established under “Definition of C-set” on page 13), that $x^p + y^p \not\equiv z^p \pmod{q}$, 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 $U_1, U_2, U_3, \dots, U_{q-1}$, where q is the largest prime $< p$. We have now computed $U_1, U_2, U_3, \dots, U_{q'-1}$, for each prime $q' < p$.

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

$$\begin{aligned} x^k &\equiv x^p \pmod{q}, \\ y^k &\equiv y^p \pmod{q}, \text{ and} \\ z^k &\equiv z^p \pmod{q}. \end{aligned}$$

By “Fermat’s Little Theorem” on page 10, 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 in Part (1) shows that for each k , $U_k > 2 \cdot 3 \cdot 5 \cdot p$ 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

$$x^k + y^k - z^k \equiv x^p + y^p - z^p \pmod{q},$$

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

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

R must be positive because, by Lemma 1.5 in Part (1), $x^k + y^k - z^k$ 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, a, b, c)" on page 31..

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 $\langle u^r + v^r, w^r \rangle$. However, we can also apply "(1.91) (c)" on page 10, namely, we can hold the exponent p fixed and investigate ordered pairs $\langle a^p + b^p, c^p \rangle$ which are congruent, as defined for C-sets, to the counterexample ordered pair $\langle x^p + y^p, z^p \rangle$.

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 $f \equiv j \pmod{m}$ and such that $h + i = j$. For example, consider the equality $25 + 15 = 40$. We find that $25 \equiv 3$, $15 \equiv 4$, and $40 \equiv 7 \pmod{11}$, 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 $z^p \equiv t \pmod{m}$ 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 in Part (1).

But "(1.91) (c)" on page 10 guarantees us that for each $a \equiv x$, $b \equiv y$, and $c \equiv z \pmod{m}$, including those a, b, c such that $a + b$ and c are each less than m , it is the case that $a^p + b^p \equiv c^p \pmod{m}$. 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 $a^p + b^p \equiv c^p \pmod{m}$, then $a + b$

$\equiv c \pmod{m}$.

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 14. 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,

$$1u \equiv a_1 \pmod{m};$$

$$2u \equiv a_2 \pmod{m};$$

$$3u \equiv a_3 \pmod{m};$$

...

$$mu \equiv a_m \pmod{m};$$

$$(m + 1)u \equiv a_{m+1} \pmod{m};$$

$$(m + 2)u \equiv a_{m+2} \pmod{m};$$

$$(m + 3)u \equiv a_{m+3} \pmod{m};$$

...

where the a_i are minimum residues mod m .

Then by a basic fact of congruence theory, $a_1, a_2, a_3, \dots, a_m$ 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 $\langle nx^p + ny^p, nz^p \rangle$, where n is a positive integer.

(D) If x, y, z are constituents of a counterexample, then by Lemma 0.0 in Part (1), $x + y > z$. It follows from (B) that

$$(1)$$

$$1x + 1y > 1z;$$

$$2x + 2y > 2z;$$

$$3x + 3y > 3z;$$

$$\dots$$

$$nx + ny > nz;$$

$$\dots$$

By Lemma 0.0 in Part (1), we know that $x + y = z + Kdef$, and so we can write, from (1),

$$(2)$$

$$1x + 1y = 1z + 1Kdef;$$

$$2x + 2y = 2z + 2Kdef;$$

$$3x + 3y = 3z + 3Kdef;$$

$$\dots$$

$$nx + ny = nz + nKdef;$$

$$\dots$$

(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! *This would not be true if the content of each cell were a randomly chosen number.* 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 cannot seriously imagine a professional mathematician saying, prior to Wiles’ proof of FLT, things like, “Well, of course we know that $17^7 + 18^7 \neq 19^7$, because $17^7 + 18^7 - 19^7 = 128,686,966$, but if a counterexample is proved to exist, then this might change, i.e., $17^7 + 18^7 - 19^7$ might no longer equal 128,686,966!” 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 in Part (1)) 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.

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 \mathbf{C} -sets whose base element is $\langle x^p + y^p, z^p \rangle$. See ““Consequences” of a Counterexample” on page 14.

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 in Part (1), $x^{p - 1} + y^{p - 1} - z^{p - 1} \geq Kdef + p - 2$, we ask if our Conjecture, if true, implies a contradiction.

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

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

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:

- “ \equiv ” means that u_k is a multiple of m_i , or, in other words, that $x^k + y^k \equiv z^k \pmod{m_i}$;
- “ $\sim\equiv$ ” means that u_k is a *not* a multiple of m_i , or, in other words, that $x^k + y^k$ is *not* $\equiv z^k \pmod{m_i}$;
- “ $\parallel c$ ” means that $\langle x^k + y^k, z^k \rangle$ is congruent to the counterexample element $\langle x^p + y^p, z^p \rangle \pmod{m_i}$, or, in other words, that $\langle x^k + y^k, z^k \rangle$ and $\langle x^p + y^p, z^p \rangle$ are in the same C-set mod m_i ;
- “ $\parallel\sim c$ ” means that $\langle x^k + y^k, z^k \rangle$ is *not* congruent to $\langle x^p + y^p, z^p \rangle \pmod{m_i}$, or, in other words, that $\langle x^k + y^k, z^k \rangle$ and $\langle x^p + y^p, z^p \rangle$ are *not* in the same C-set mod m_i ;

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

- “ \equiv ”, “ $\parallel c$ ”, or
- “ $\sim\equiv$ ”, “ $\parallel\sim c$ ”, or
- $\sim\equiv$, “ $\parallel\sim c$ ”.

(We use “ \parallel ” because it suggests the “vertical congruence” imposed by Fermat’s Little Theorem.)

No cell can contain the pair $\langle \sim\equiv, \parallel c \rangle$, because that would mean that $\langle x^p + y^p, z^p \rangle$ 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 “ \equiv ” 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 $x^p + y^p \equiv z^p \pmod{m_i}$ for all i and therefore each cell in the u_p row contains $\langle \equiv, \parallel c \rangle$.

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 $\langle \equiv, \parallel c \rangle$. The reason is that, for each m_i , there is a (congruent) C-set containing the element $\langle x^p + y^p, z^p \rangle$, and since a C-set contains an infinity of elements, an infinity of cells must contain $\langle \equiv, \parallel c \rangle$.

We also remind the reader of the facts concerning an infinite succession of prime moduli, q, q^2, q^3, \dots , as discussed under ““Consequences” of a Counterexample” on page 14.

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 $\langle \equiv, \|\|c \rangle$ 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 $U(k, a, b, c)$

See “Appendix B — Approach Via the Fixed Set” on page 32.

Appendix B — Approach Via the Fixed Set

Definitions

For the reader's convenience, we here repeat several definitions that were given in Part (1) of this paper, and above in this Part.

Definition of “Minimum Counterexample”

Assume a counterexample exists. Without loss of generality, we can assume that x, y, z are relatively prime in pairs, i.e., that

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

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

(1.85) Without loss of generality, it suffices to prove FLT for every odd prime $p \geq 3$. (See “(1.85): Statement and Proof” on page 5.)

Assuming that there exists x, y, z, n , where n is an odd prime, such that $x^n + y^n = z^n$. Then, without loss of of generality, we let $n = p$, the smallest such odd prime. We will write p instead of n when referring to an assumed counterexample.

If there is more than one triple $\langle x, y, z \rangle$ such that x, y, z are elements of a counterexample¹ with exponent p , then we choose the $\langle x, y, z \rangle$ having the minimum x . If there is more than one such triple, then we choose the $\langle x, y, z \rangle$ having the minimum y . Clearly, there can only be one such triple. We call that triple, and exponent p , the *minimum counterexample*. From now on in this paper, unless stated otherwise, the term “counterexample” will always mean “minimum counterexample”.

“Lemma 4.0.5: Statement and Proof” on page 28 shows that, for given x, y, z , there can be at most one prime p such that $x^p + y^p = z^p$.

Definition of $U(r, a, b, c)$

Let r, a, b, c , be positive integers. Then we define $U(r, a, b, c)$ to be equal to $a^r + b^r - c^r$.

Definition of Fixed-set F

We begin with some examples.

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

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

Prior to Wiles' proof, namely, in the early 90s, FLT had been proved for all prime exponents

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

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

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

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

(2) the set $\sim F$, the complement of F .

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

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

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

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

Some Other Elements of the Fixed-set F

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

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

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

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

...

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

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

Some Other Elements of $\sim F$

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

The Approach

We give two implementations of the Approach.

First Implementation

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

$$\begin{aligned} &U(1, x, y, z), \\ &U(2, x, y, z), \\ &U(3, x, y, z), \end{aligned}$$

....

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

Second Implementation

By basic algebra, it is easy to show that

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

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

$$(2)$$

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

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

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

Remark 1

The skeptical reader may be inclined to argue that all we have shown is that either $U(p, x, y, z)$ is a counterexample or it is not — in other words, that it can't have two values. We disagree. Obviously, $U(p, x, y, z)$ has only one value. The question is, can that value have any influence on the value of $U((p-1), x, y, z)$? If yes, then we have a contradiction and a proof of FLT. On the other hand, if the values of all $U(r, a, b, c)$ except $U(p, x, y, z)$ were each chosen at random, or were all equal to the same constant c , then the fixed set F would contain *all* $U(r, a, b, c)$ *except* $U(p, x, y, z)$.

A more direct proof would use the value of $U((p-1), x, y, z)$ to show that $U(p, x, y, z)$ cannot be an integer, and thus cannot be a counterexample. See “Vertical Approach Using the Calculus” in Part (1) of this paper, on occampress.com.

Remark 2

We challenge the skeptical reader to prove that it is possible for $x^{p-1} + y^{p-1} - z^{p-1} = U((p-1), x, y, z)$ to remain unchanged regardless if $x^p + y^p - z^p = 0$ or not. Such a proof would, of course, negate our strategy above.

Remark 3

The fixed-set strategy also seems applicable to a proof of the $3x + 1$ Conjecture. See “Proof of the $3x + 1$ Conjecture” in “A Solution to the $3x + 1$ Problem” on www.occampress.com.

The Concept at the Heart of This Approach

The heart of our Strategy is the fact that a counterexample “has consequences”. The briefest explanation I can give of what this means is the following: let S be a 4-dimensional space in which each point is a 4-dimensional cube, with all cubes being the same size. The cube having coordinates (r, a, b, c) contains $U(r, a, b, c)$. It should be immediately clear that if c is a cube, then the value in each adjacent cube is related to the value of c , where an *adjacent cube* is one in which just one coordinate differs from the corresponding coordinate of c . In fact, we can compute the value of the adjacent cube *from* the value in c . So if the value in c is 0 (which would be the case if a counterexample to FLT existed), then the values in adjacent cubes will differ from what they would be if the value in c were not 0. This is what I mean when I say that a counterexample “has consequences”.

As we said in the section, “Some Other Elements of the Fixed-set F” on page 33, if the value

of each $U(r, a, b, c)$ were chosen at random, then a counterexample would *not* have consequences, because the value in each cube adjacent to a cube c that contained 0, would have no relationship to 0. We could not determine this value *from* the value 0.

For further details, see the section ““Consequences” of a Counterexample” on page 14 and also the section “Four-Dimensional Approach” in Part (1) of the same paper. This latter section discusses the possibility of “crooked induction” from the cube that contains an assumed counterexample.