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

Part (4)

Three Promising Approaches

Plus

Details on "Vertical" Approaches in General

by

Peter Schorer

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

Sept. 18, 2020

Key words: Fermat's Last Theorem

Overview of This Part

The Fundamental Idea

This Part is based on the following fundamental idea:

1. Assume a counterexample $x^p + y^p = z^p$ to Fermat's Last Theorem (FLT) exists, and assume it is the minimum counterexample[1], which means, among other things, that p is the smallest prime in any counterexample. (It is well known that we only need consider prime exponents in assumed counterexamples.)

2. Now consider the set of all $U(k, x, y, z) = x^k + y^k - z^k$, where $k \geq 1$. For each prime modulus q such that $(x, q) = (y, q) = (z, q) = 1$, the set of all $U(k, x, y, z)$ can be partitioned into sets of congruent $U(k, x, y, z)$ mod q. (The exponents k of these congruent $U(k, x, y, z)$ are congruent mod $(q - 1)$.)

3. We attempt to derive a contradiction from the fact that $U(p, x, y, z)$ is the only $U(k, x, y, z)$ that equals 0. The Fixed-Set concept (described below in this section under "The Fixed-Set" on page 3), has been our most promising means of accomplishing this.

Our best effort to obtain a proof based on this strategy is "Appendix A — Third Promising Approach to a Simple Proof of FLT" on page 68.

An Earlier Form of the Fundamental Idea

In earlier work in this Part (for example in the sections on C-Sets and D-sets), we considered, not the set of all $U(k, x, y, z)$, but the set of all 2-tuples $<x^k + y^k,\ z^k>$. Here, although for all k except p, $x^k + y^k \neq z^k$, the left-hand and right-hand elements of a 2-tuple are congruent or not congruent depending on the prime modulus q.

For each prime modulus q, the set of all $<x^k + y^k,\ z^k>$ can be partitioned into sets of congruent 2-tuples $<x^k + y^k,\ z^k>$. By *congruent 2-tuples* we mean 2-tuples $<x^k + y^k,\ z^k>$, and $<x^{k'} + y^{k'},\ z^{k'}>$ such that $x^k \equiv x^{k'} \bmod q$, $y^k \equiv y^{k'} \bmod q$ and $z^k \equiv z^{k'} \bmod q$. The exponents k of these 2-tuples are congruent mod $(q - 1)$. If two 2-tuples are congruent, then if the elements of one such tuple are congruent mod q, so must the elements of the other tuple be congruent. And similarly, if the elements of one such tuple are not congruent mod q, then so must the elements of the other tuple not be congruent.

We attempted to derive a contradiction from the fact that, if, for some prime modulus q, the first and second elements of each 2-tuple were not congruent mod q for $1 \leq k \leq q - 1$, and $q - 1$ were less than p, then we would have a proof of FLT, because the elements of all the 2-tuples of each congruent set would have to be not congruent, since the first and second elements in the first 2-tuple in each such set were non-congruent. But in the congruent set containing $<x^p + y^p,\ z^p>$ all the 2-tuples would have to be congruent, since $x^p + y^p \equiv z^p \bmod q$ for any q,. Hence we would have a contradiction that would give us a proof of FLT.

The Main Difficulty With This Earlier Form

The main difficulty with this approach is the following:

---

1. The term is formally defined in "Definition of 'Minimum Counterexample'" in Part (1) of this paper.

We can be assured that $x^k + y^k$ not $\equiv z^k \bmod q$ if we choose a modulus q such that $max(x^k + y^k, z^k > < q$. For, in general, if $max(a + b, c) < m$, where m is any modulus, and if $a + b \neq c$, then, by definition of congruence, $a + b$ not $\equiv c \bmod m$.

However, it might be that there does not exist a prime modulus q such that:

$max(x^k + y^k, z^k >$ is less than $q < p$ for all k where, $1 \leq k \leq q - 1$. Then we do not have our necessary non-congruent first 2-tuple in each of the congruent sets for $1 \leq k \leq q - 1$. And thus, we would not have our desired contradiction.

We should not fail to mention the original version of the Earlier Form. There, we began with the realization that if a positive integer exists — for example, the positive integers $x^p + y^p$ and z^p — then there must exist a prime modulus q such that for all prime moduli $\geq q$, the positive integer must be less than q. We then attempted to show that the counterexample 2-tuple would always be kept greater than q, for all q, which would have been a proof that the counterexample did not exist. We made no headway with this approach.

What we regard as our most promising approaches are those that use the Fixed-Set.

The Fixed-Set

We cannot seriously imagine a professional mathematician saying, prior to Wiles' proof of FLT, things like, "Well, of course we know that $17^3 + 6^3 - 19^3 = -1730$, not 0, but if a counterexample is proved to exist, then this might change — the value on the right-hand side might no longer be 1730."

Thus, we say that $17^3 + 6^3 - 19^3 = U(3, 17, 6, 19)$ is an element of the *Fixed-Set F*, because the value of $17^3 + 6^3 - 19^3$ 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 (and hence for all exponents) less than 4,000,000. The Fixed-Set *F includes* all $U(k, a, b, c)$ such that $k < p$, where p is the assumed (prime) exponent in the minimum counterexample. In particular, it includes all $U(k, x, y, z)$, where $k < p$ 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 $U(k, a, b, c)$ into two sets:

(1) the set $F = \{U(k, a, b, c) \mid a^k + b^k - c^k$ is the same regardless whether a counterexample exists or not (for this reason, we call F 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, $U(k, a, b, c) \neq 0$)." (In fact, it is easy to show that if a counterexample exists, there is an infinity of $U(k, a, b, c)$ that are not in the Fixed-Set.)

All three of our most promising Approaches to a simple proof of FLT make use of the Fixed-Set concept. See "Three Promising Approaches to a Simple Proof of Fermat's Last Theorem" on page 4

Three Promising Approaches to a Simple Proof of Fermat's Last Theorem

In this section, we collect, and make as clear and easy-to -understand as possible, three approaches to a simple proof of FLT that are contained elsewhere in this Part. (Thus, there is a certain amount of duplication in this Part.)

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

We define $U(k, a, b, c)$, where k, a, b, c are positive integers, to be $a^k + b^k - c^k$, which we sometimes call the *value* of $U(k, a, b, c)$, not to be confused with the *location* of $U(k, a, b, c)$, which is defined in the same way as the location of $U(k, x, y, z)$ (see "Definition of "Location" of U(k, x, y, z)" on page 8).

Definition of "Counterexample" and of *U*(*k*, *x*, *y*, *z*)

If there exist positive integers x, y, z, p, where p is prime and x, y, z are relatively prime in pairs, such that $x^p + y^p = z^p$, then $x^p + y^p = z^p$ is a counterexample (to FLT). We assume that p is the smallest exponent in any counterexample, and, in fact that $x^p + y^p = z^p$ is a *minimal counterexample*, as defined in Part (1) of this paper. Since x, y, z are relatively prime in pairs, we do not have to consider separately the possibility that p is a factor of x or y or z.

Clearly, if $x^p + y^p = z^p$, then $U(p, x, y, z) = 0$.

We remark in passing that each $U(k, x, y, z)$ is a point on the curve $f(k) = x^k + y^k - z^k$ as defined in the section "First Vertical Approach Using the Calculus" in Part (1) of this paper, on occampress.com.

First Promising Approach

Definition of Fixed-Set *F*

We begin with an example.

We cannot seriously imagine a professional mathematician saying, prior to Wiles' proof of Fermat's Last Theorem (FLT), things like, "Well, of course we know that $17^3 + 6^3 - 19^3 = -1730$, not 0, but if a counterexample is proved to exist, then this might change — the value on the right-hand side might no longer be -1730."

Thus, we say that $17^3 + 6^3 - 19^3 = U(3, 17, 6, 19)$ is an element of the *Fixed-Set F*, because the value of $17^3 + 6^3 - 19^3$ 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 (and hence for all exponents) less than 4,000,000. 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. 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 $U(k, a, b, c)$ into

two sets:

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

It is clear from what we have said that our Fixed-Set *includes* at least the set $\{U(1, x, y, z), U(2, x, y, z), \mathrm{U}(3, x, y, z), ..., U(p - 1, x, y, z)\}$.

First Possible Proof of FLT[1]

By basic algebra, it is easy to show that there exists a $g(x, y, z)$ such that

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

where $g(x, y, z)$ is an algebraic expression involving products of powers of x, y, z. In fact, if we multiply out the product on the left-hand side of (1), we get $x^p + y^p - z^p$ + (a set of terms which we call $(g(x, y, z))$), yielding Equation (1). It follows that:

(2)
$$x^{p-1} + y^{p-1} - z^{p-1} = (x^p + y^p - z^p - \mathrm{g}(x, y, z))/(x + y + z).$$

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 (if our reasoning is correct) FLT is proved.

A Variation of the First Possible Proof of FLT

For each k, where $3 \leq k \leq p$, $z^k - y^k \neq x^k$. All these $z^k - y^k$ are elements of the Fixed-Set.

But for p, by assumption of a counterexample, $z^p - y^p = x^p$. Each prime factor of $z^p - y^p$ must be a power of p. Clearly, $z^p - y^p$ is not an element of the Fixed-Set.

Now z^{p-1} is certainly an element of the Fixed-Set. (Its value is the same whether or not a counterexample exists.) But then so is $z \cdot z^{p-1} = z^p$ (z is an element of the Fixed-Set, and the

1. This is "First Version of Fixed-Set Approach" on page 36

rules of multiplication are not subject to the existence or non-existence of a counterexample.)

Similarly for y^p.

But then $z^p - y^p$ must likewise be an element of the Fixed Set, which is a contradiction. If our reasoning is valid, we have a proof of FLT.

Another Variation of the First Possible Proof of FLT

A basic algebraic fact is that for all $k \geq 3$,

(1)
$$d^k - c^k = (d - c)(d^{k-1} + cd^{k-2} + c^2d^{k-3} + ... + c^{k-1}),$$

and therefore for x, y, z in our assumed counterexample, we have for all $k \geq 3$,

(2)
$$z^k - y^k = (z - y)(z^{k-1} + yz^{k-2} + y^2z^{k-3} + ... + y^{k-1}).$$

Of course, within this range of exponents,

(3)
$$z^k - y^k = (z - y)(z^{k-1} + yz^{k-2} + y^2z^{k-3} + ... + y^{k-1}) \neq x^k.$$

However, for $k = p$, by assumption we have

(4)
$$z^p - y^p = (z - y)(z^{p-1} + yz^{p-2} + y^2z^{p-3} + ... + y^{p-1}) = x^p.$$

This means that each prime factor of $z^p - y^p$ must be a power of p, and similarly for each prime factor of $(z - y)(z^{p-1} + yz^{p-2} + y^2z^{p-3} + ... + y^{p-1})$ x^p and similarly for each prime factor of x^p. Furthermore, the set of prime factors for each of the three terms must be the same.

Now consider $(z - y)$. By statement (4) each of its prime factors must be either a power of p, or a power r such that there is a prime factor in $(z^{p-1} + yz^{p-2} + y^2z^{p-3} + ... + y^{p-1})$ raised to the power s such that $r + s = p$. There can obviously be no change in the value of $(z - y)$ in the transition from (3) to (4) because $(z - y) = (z - y)$ (always!). So we must consider $(z^{p-2} + yz^{p-3} + y^2z^{p-4} + ... + y^{p-2})$, which is the factor in the case for $k = p - 1$.

This factor is the same whether or not a counterexample exists, because it is a factor in an exxpression in the Fixed-Set, namely the expression, $(z - y)$ $(z^{p-2} + yz^{p-3} + y^2z^{p-4} + ... + y^{p-2})$. If we multiply it by z, the result, $z(z^{p-2} + yz^{p-3} + y^2z^{p-4} + ... + y^{p-2})$ will be the same whether or not a counterexample exists. If we then add y^{p-1} to $z(z^{p-2} + yz^{p-3} + y^2z^{p-4} + ... + y^{p-2})$ the result, $z(z^{p-2} + yz^{p-3} + y^2z^{p-4} + ... + y^{p-2}) + y^{p-1}$ will still be the same whether or not a counterexample exists.

But now we have obtained the factor $(z^{p-1} + yz^{p-2} + y^2z^{p-3} + ... + y^{p-1})$, which is a factor of $(z - y)(z^{p-1} + yz^{p-2} + y^2z^{p-3} + ... + y^{p-1})$, which equals $z^p - y^p = x^p$, In other words, our counterexample is in the Fixed-Set, which is a contradiction brought about by our assumption that $x^p + y^p = z^p$ is a counterexample. Therefore a counterexample does not exist. If our reasoning is correct, we have a proof of FLT.

Second Promising Approach

Definition of "Congruent Set"

Let q be an odd prime. Then the following sets of congruent $U(k, x, y, z)$ exist. We call each such set a *congruent set mod q*, or, if q is understood, then simply a *congruent set*.

$\{U(k, x, y, z) \mid k \equiv 1 \bmod q - 1\}$,
$\{U(k, x, y, z) \mid k \equiv 2 \bmod q - 1\}$,
...
$\{U(k, x, y, z) \mid k \equiv q - 1 \bmod q - 1\}$,

Proof That Congruent Sets Exist

(**Step A.1**)
If q is an odd prime and u is a positive integer, then $u^r \equiv u^{r + j(q-1)} \bmod q$, where $r \geq 1, j \geq 0$.
Proof of step (A.1):
There are two cases: (I) $(u, q) = 1$ and (II) $(u, q) \neq 1$.

Case I:
By Fermat's Little Theorem, we know that $1 \equiv u^{q-1} \bmod q$. The result follows by repeated multiplying of both sides of the congruence by u. □

Case II:
If u and q have a factor in common, that factor must be q. Therefore, by definition of the integers mod q, u is congruent to all multiples of q. Thus, in particular, $u^1 \equiv u^{1+q-1} \bmod q$, The result follows by repeated multiplying both sides of the congruence by u. □

(**Step A.2**)
It follows from (Step A.1) that

$$x^i \equiv x^{i+j(q-1)} mod \ \ q$$

$$y^i \equiv y^{i+j(q-1)} mod \ \ q$$

$$z^i \equiv z^{i+j(q-1)} mod \ \ q$$

where $j \geq 0$, and $1 \leq i \leq q - 1$. Therefore, by a basic fact of congruence theory, $U(i, x, y, z) \equiv U(i +$

$j(q-1), x, y, z) \bmod q$.

We call $U(i, x, y, z)$, where $1 \le i \le q-1$, the *base element* of its congruent set. The successive values of the $U(i, x, y, z)$ can "jump around": some may be positive, some negative, one may be zero. The term base element refers only to the location of $U(i, x, y, z)$ relative to other $U(k, x, y, z)$.

We call the set $\{U(i + j(q-1), x, y, z)\}$, where $1 \le i \le q-1$ and j is constant, a *row* in the set of all congruent sets mod q.

Definition of "Location" of $U(k, x, y, z)$

For each prime modulus q, each $U(k, x, y, z)$ — including $U(p, x, y, z)$ — has a *location* in the set of congruent sets mod q. A *location* is defined by the ordered pair (i, row), where i is the exponent of the base element of a congruent set — thus $1 \le i \le q-1$ — and *row* is the value of j in $k = i + j(q-1)$, where $j \ge 0$. In other words, i is the remainder of $k/(q-1)$, and *row* is the quotient of $k/(q-1)$. A congruent set mod q is therefore the set of all $U(k, x, y, z)$ such that, for some i, where $1 \le i \le q-1$, $k \equiv i \bmod (q-1)$.

The location of $U(k, x, y, z)$ is the same whether or not a counterexample exists. Even though the *value* of a $U(k, x, y, z)$ may differ, depending on whether a counterexample exists or not, the *location* of $U(k, x, y, z)$ does not differ.

A Few Properties of Congruent Sets

The set of congruent sets mod q is the same, regardless if a counterexample exists or not. Thus, regardless if a counterexample exists or not, for $q < p$, the element $U(p, x, y, z)$ is *not* a base element even though its value is 0. For all $q \ge p$, $U(p, x, y, z)$ *is* a base element.

Since, if a counterexample exists, $U(p, x, y, z) \equiv 0 \bmod q$, it follows that all elements in the congruent set containing $U(p, x, y, z)$ — whether or not $U(p, x, y, z)$ is the base element — are likewise congruent to 0 mod q — that is, are multiples of q. Hence the base element cannot be relatively prime to q.

We emphasize that ongruent sets merely establish *congruences* between $U(k, x, y, z)$ mod q. Congruent sets do not determine the *values* of the $U(k, x, y, z)$, because to say that $u \equiv v \bmod m$ is to say only that u and v differ by some multiple of m. It is not to say what the actual values of u and v are. Thus the *values* of the $U(k, x, y, z)$ in a given congruent set are all congruent, hence are all elements of one congruence class mod q, but they are in general not in the same *order* (increasing order) as the elements of a congruence class normally are.

A collection of facts about $U(k, x, y, z)$ and congruent sets that are not needed for this Approach to a possible proof of FLT, can be found in "Basic Facts About U(k, x, y, z) And Congruent Sets" on page 21.

Second Possible Proof of FLT[1]

1. If $U(p, x, y, z)$ is not a counterexample, then it is a finite product of primes. Thus there is an infinity of primes q (we don't know which ones) such that $U(p, x, y, z)$ is in a congruent set mod q such that $U(p, x, y, z)$ is not a multiple of q. Nor is any $U(p + j(q-1), x, y, z)$ a multiple of q, where j is a positive or negative integer.

1. This is "Fourth Version of Fixed-Set Approach" on page 37

2. But what we have said does not apply if $U(p, x, y, z) = 0$. In that case, for each prime modulus q, $U(p, x, y, z)$ is an element of the congruence *class* all of whose elements are multiples of q. So, trivially, $U(p + j(q - 1), x, y, z)$, where j is a positive or negative integer, is a multiple of q.

3. But this means that some members of the Fixed-Set F are also in the complement of that Set, which is a contradiction. These members are the $U(p + j(q -1), x, y, z)$, where j is a negative value that still leaves a positive exponent. Since these exponents are less than p, they are members of the Fixed-Set. When a counterexample did not exist, they were not a multiple of q, but when a counterexample exists, they are. If our reasoning is correct, this contradiction gives us a proof of FLT.

Third Promising Approach

This Approach is described in "Appendix A — Third Promising Approach to a Simple Proof of FLT" on page 68.

The remainder of this Part (that is, Part (4) of our paper) consists of (1) material that led to the above three promising approaches to a simple proof of FLT; and (2) other material leading to other at present less-promising approaches.

Definition of "Vertical" Approach

We quote from the section, "Why Should We Hold Out Any Hope That a "Simple" Proof Exists?" in Part (1) of this paper, on occampress.com.

> Most of the research on FLT over the more than three centuries prior to Wiles' proof centered on expanding the size of the exponent n for which FLT is true. We can call this strategy the "Horizontal Approach", because for each n the goal is to prove that FLT is true for all x, y, z, here imagined as constituting a "horizontal" set relative to the "vertical" direction of progressively increasing n.
> But there is another approach, one that we call the "Vertical Approach". Here, we assume that x, y, z are elements of a counterexample to FLT, then we attempt to find the n such that $x^n + y^n = z^n$ proceeding from $n = 3$ to $n = 4$ to $n = 5$, etc., i.e., proceeding in the "vertical" direction of progressively increasing n relative to the fixed x, y, z. If we can show that we can never "get to" such an n for any x, y, z, or that the assumption that for some n, $x^n + y^n = z^n$ leads to a contradiction, then we will have a proof of FLT.

Underlying all of our "Vertical" Approaches has been a geometric view of congruence. It is described under "Definition of "Lines-and-Circles" Model of Congruence" on page 10.

We now believe that one reason that a proof of FLT and a solution to the 3x + 1 Problem are so notoriously difficult is that the behavior of the counterexample case is so similar to the behavior of the non-counterexample case. By this we mean the following. Each finite sequence of iterations of the $3x + 1$ function can be represented by a finite tuple. All tuples that are related in a cer-

tain elementary way are collected in a tuple-set. Lemma 2.0 in our paper states that if a counterexample to the $3x + 1$ Conjecture exists, then each tuple-set (there is a countable infinity of tuple-sets) contains an infinity of counterexample tuples *and* an infinity of non-counterexample tuples. This Lemma expresses what we mean when we say that the behavior of the counterexample case is so similar to the behavior of the non-counterexample case.

In this Part of our FLT paper we define what we can call the *FLT function*. It is simply $a^k + b^k - c^k$, where a, b, c, k are positive integers. If a counterexample $x^p + y^p = z^p$ exists — so that $x^p + y^p - z^p = 0$ — then $x^k + y^k - z^k$, where $k \geq 1$, is clearly a sub-function of the FLT function. We have as yet no lemma for the FLT function that is equivalent to our Lemma 2.0 for the $3x + 1$ function, but the stubborn refusal of attempts at a proof by contradiction of FLT are similar to the stubborn refusal of attempts in connection with the $3x + 1$ Conjecture. The practice among many, pehaps most, $3x + 1$ researchers, has been to generate ever more results describing the behavior of the $3x + 1$ function in hopes that the way to a proof of the Conjecture will sooner or later appear. Similarly, we have generated many results concerning the behavior of the Fermat function in hopes that a proof of FLT will appear. We now consider such efforts doomed to failure not only because, as we mentioned at the start of this section, the behavior of the counterexample case is so similar to the behavior of the non-counterexample case, but also because "local" approaches to a proof of FLT do not seem to work. To quote from (3) under "Why Is It So Difficult to Prove FLT?" in Part (1) of this paper, on occampress.com:

> An example of what we mean by a 'local' approach is a standard proof by contradiction. We assume that a counterexample to FLT exists, and try to derive a contradiction. We are working 'locally' because we are considering only the counterexample and what we can deduce by, say, algebraic operations based on it. However, it seems that a contradiction always evades us, either because we find that we need information that we do not possess... or because the crucial property that we hope will give us a contradiction is shared by a non-counterexample as well.

The most-promising strategy mentioned at the start of this section is based on a *comparison strategy*, in which the behavior of the FLT function if a counterexample exists is compared with the behavior of the function if a counterexample does not exist. The reader will not be surprised to learn that the strategy is controversial. We attempt to refute several of the more frequent objections in preliminary remarks in "Approach Via Fixed-Set" on page 33. A more extensive refutation is given in item (3) under "Important Preliminary Remarks" in our $3x + 1$ paper, and in a separate short paper, "Is It Legitimate to Begin a Sentence With 'If a Counterexample Exists, Then ...'" on occampress.com.

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

Virtually all of our "Vertical" 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).

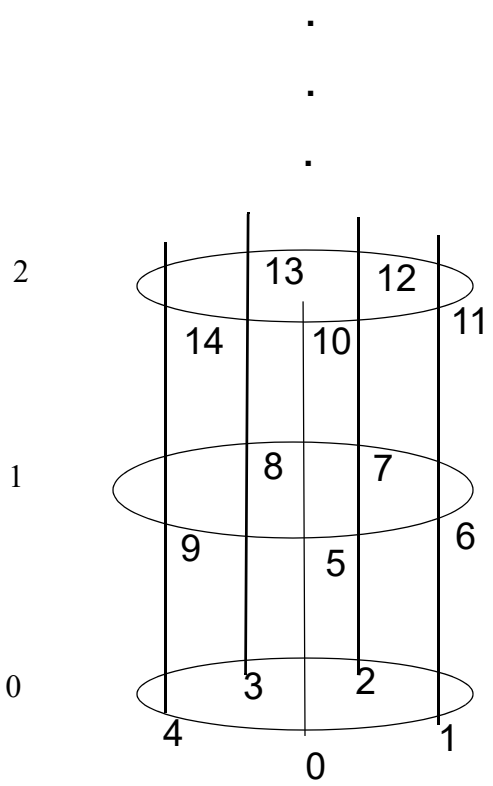

Fig. 1. "Geometrical" model of positive integers congruent mod 5.

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 of line 4. We sometimes refer to level 0 as the *base level mod m* (or merely the *base level* when m is understood).

Definition of "Location" of a Positive Integer

The *location* of a positive integer is similar to the location of $U(k, x, y, z)$ (see "Definition of "Location" of U(k, x, y, z)" on page 8). For each modulus m, each positive integer u has a *location* relative to that modulus. This location is given by the ordered pair [*line, level*], which can be regarded as the "address" of u mod m. Thus, in the example in the previous section, the address of 14 mod 5 is given by [4, 2]. In the course of this Part, we will be concerned with the terms $a^k + b^k - c^k$, where a, b, c, k are positive integers, and we will be specifically concerned with $x^k + y^k - z^k$, where x, y, z are elements of an assumed counterexample. In older sections of this Part, namely, in "Approaches Via D-Sets" on page 47 and in "Approaches Via C-Sets" on page 49, we will be concerned with ordered triples $<a^k, b^k, c^k>$, $<x^p, y^p, z^p>$, where $x^p + y^p = z^p$ is an assumed minimum counterexample, and with all $<x^k, y^k, z^k>$, where $k \geq 1$. In all these cases, we think of each

term or tuple as representing a location in a lines-and-circles model.

Definition of "Touches Down"

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 "Congruent Ordered Triples"

Let $<u, v, w>, <u', v', w''>$ 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 $w \equiv w'$ mod m, we say that the *ordered triples are congruent mod m* and that $<u, v, w>$ *is congruent to* $<u', v', w''>$ *mod m*. We will omit *mod m* when m is understood. For a triple $<u, v, w>$ there are two possibilities: $u + v \equiv w$ mod m, or $u + v$ not $\equiv w$ mod 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

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

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

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

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

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

After a great deal of effort, we have been unable to make this strategy work, although it is dicussed at length in the section, "Approaches Via C-Sets" on page 49. The strategy has, however, motivated other approaches that are described in this Part of our paper.

Appropriate and Non-Appropriate Moduli

An *appropriate modulus* is a modulus m such that $(x, m) = (y, m) = (z, m) = 1$. We have recently come to the tentative conclusion that it is not necessary for us to consider appropriate moduli. The reason is made clear in "Statement (A)" on page 20, in the section "Approaches Using Only Powers of x, y, z (Congruent Sets)" on page 19.

Appropriate Moduli

We know:

- There is a countable infinity of appropriate moduli (because there is a countable infinity of primes larger than the largest prime in x, y, or z).
- Each factor of an appropriate modulus is an appropriate modulus.
- Each product of appropriate moduli is an appropriate modulus. However, the product of an appropriate modulus and a non-appropriate modulus, is a non-appropriate modulus.

Non-Appropriate Moduli

We know:

- There are only a finite number of *prime* non-appropriate moduli (because all primes larger than the largest prime in x, y, z are appropriate moduli).
- Each factor of a non-appropriate modulus is a non-appropriate modulus.
- Each product of non-appropriate moduli is a non-appropriate modulus, as is each product of a non-appropriate modulus and an appropriate modulus.
- There is a countable infinity of non-appropriate moduli (because by the previous fact, there is an infinity of products of non-appropriate moduli).

What We Need in Appropriate Moduli

Our needs, when it comes to appropriate moduli, are somewhat conflicting. On the one hand, we need an appropriate modulus m that is small relative to x, y, and z. The reason is that this will enable us to have many terms $x^j + y^j$, $a^j + b^j$, and $a^p + b^p$ each congruent to, but less than, $x^p + y^p$ mod m, and many terms z^j, c^j, and c^p each congruent to, but less than z^p, as required by "1st Condition for Truth of FLT" on page 15, "2nd Condition for Truth of FLT" on page 16, and "3rd Condition for Truth of FLT" on page 17, respectively. (Of course, no modulus can be less than 2.)

On the other hand, we need the modulus m to be large enough so that each of the pair $x^j + y^j$, and z^j, is less than m, and similarly for each of the pair $a^j + b^j$, and c^j, and for each of the pair $a^p + b^p$, and c^p .

Approaches Using Powers of a, b, c

In all cases, $x^p + y^p = z^p$ is the assumed (minimum) counterexample. The prime modulus q in the following is an appropriate modulus. Equivalent conditions apply to composite moduli.

Outline of These Approaches

The following is an attempt to convey to the reader the idea underlying all the approaches in this section. We will mark with "[1]", "[2]", ... etc., the end of each statement that is unproved or invalid. The explanation for each [i] is given below our argument.

In the table[1] below,
q is a prime modulus, with $q < p$, the exponent in an assumed counterexample.
$a \equiv x \bmod q$ and $a < q$; $b \equiv y \bmod q$ and $b < q$; $c \equiv z \bmod q$ and $c < q$.

We argue as follows:

1. $p = i + j(q - 1)$ for some i, $1 \le i \le q - 1$. Therefore, $<x^p + y^p, z^p>$ is in a row in the table that

1. The x, y, z terms in each column correspond to the terms in a congruent set. See "Definition of "Congruent Set"" on page 19

is above the lowest row.

2. Since by assumption $x^p + y^p = z^p$, $x^p + y^p \equiv z^p \bmod q$.

3. The bottom element in the column containing $<x^p + y^p, z^p>$ is $<a^i + b^i, c^i>$. Since $a^i + b^i \neq c^i$ (because equality would imply a counterexample smaller than the minimum counterexample), it follows that $a^i + b^i$ not $\equiv c^i \bmod q$ **[1]**. Therefore, by a basic fact of congruence theory, $x^i + y^i$ not $\equiv z^i \bmod q$, and by Fermat's Little Theorem, $x^p + y^p$ not $\equiv z^p \bmod q$. But this contradicts the statement in step 2, and so we have a proof of FLT.

[1] Even though it is true that if $u + v = w$, then $u + v \equiv w \bmod q$, it is not necessarily true that if $u + v \neq w$, then $u + v$ not $\equiv w \bmod q$. This non-congruence, however, is necessarily true when $u + v < q$ and $w < q$. But even though, by definition, $a < q$, $b < q$, and $c < q$, we don't know if $a + b < q$, much less if, for each i, where $1 \leq i \leq q - 1$, $a^i + b^i < q$, and $c^i < q$.

Table 1:

...	...	...	...	...
$x^{1+(q-1)} + y^{1+(q-1)}, z^{1+(q-1)}$	$x^{2+(q-1)} + y^{2+(q-1)}, z^{2+(q-1)}$	$x^{3+(q-1)} + y^{3+(q-1)}, z^{3+(q-1)}$	...	$x^{(q-1)+(q-1)} + y^{(q-1)+(q-1)}, z^{(q-1)+(q-1)}$
$a^{1+(q-1)} + b^{1+(q-1)}, c^{1+(q-1)}$	$a^{2+(q-1)} + b^{2+(q-1)}, c^{2+(q-1)}$	$a^{3+(q-1)} + b^{3+(q-1)}, c^{3+(q-1)}$	...	$a^{(q-1)+(q-1)} + b^{(q-1)+(q-1)}, c^{(q-1)+(q-1)}$
$x^1 + y^1, z^1$	$x^2 + y^2, z^2$	$x^3 + y^3, z^3$	...	$x^{q-1}+y^{q-1}, z^{q-1}$
$a^1 + b^1, c^1$	$a^2 + b^2, c^2$	$a^3 + b^3, c^3$	...	$a^{q-1}+b^{q-1}, c^{q-1}$

First Approach Using Powers of *a*, *b*, *c*

1st Condition for Truth of FLT

If there exists a prime q such that:
$(x, q) = (y, q) = (z, q) = 1$, and
$p \equiv j \bmod q - 1$, so that $x^p \equiv x^j$, $y^p \equiv y^j$, and $z^p \equiv z^j \bmod q$,
and $2 < j < p$,
and $x^j + y^j < q$ and $z^j < q$,
Then FLT is true.

Proof:

We have a contradiction that implies the truth of FLT. For, on the one hand, $x^j + y^j \equiv z^j \bmod q$, by Fermat"s Little Theorem (see Part (1) of this paper, on the web site occampress.com) and the fact that $x^p + y^p = z^p$ implies $x^p + y^p \equiv z^p \bmod q$. But on the other hand $x^j + y^j$ not $\equiv z^j \bmod q$ because $x^j + y^j \neq$ to z^j (the contrary would imply a counterxample with an exponent smaller than p), and $x^j + y^j < q$, and $z^j < q$. □

The Condition generalizes to compound moduli m via Euler's Totient Function, $\varphi(m)$.

Second Approach Using Powers of *a*, *b*, *c*

2nd Condition for Truth of FLT

If there exists a prime q such that:
$(x, q) = (y, q) = (z, q) = 1$, and
$p \equiv j \bmod q - 1$, so that $x^p \equiv x^j$, $y^p \equiv y^j$, and $z^p \equiv z^j \bmod q$,
and $2 < j < p$,
and $a \equiv x$, $b \equiv y$, and $c \equiv z \bmod q$, and
$a^j + b^j < q$ and $c^j < q$,
Then FLT is true.

Proof:

Proof of 1st Condition applies to a, b, c that are congruent to x, y, z, respectively, mod q. □

The Condition generalizes to compound moduli m via Euler's Totient Function, $\varphi(m)$.

Discussion of the 2nd Condition for Truth of FLT

It appears straightforward to show that if $u + v = w$, then for each modulus m, there exist $c \equiv u$, $d \equiv v$, and $e \equiv w \bmod m$ such that $c + d =$ e. For example, $9 + 8 = 17$. Now $4 \equiv 9$, $3 \equiv 8$, and $7 \equiv 17 \bmod 5$, and, indeed, $4 + 3 = 7$.

Fermat's Little Theorem gives us a^j, b^j and c^j congruent to x^p, y^p, and z^p respectively mod q. By a basic fact of congruence theory, there are many triples f, g, h such that $f \equiv a$, $g \equiv b$, and $h \equiv c \bmod q$ and therefore for each such triple, $f^j + g^j \equiv h^j \bmod q$. If we can show that for one of these triples, $f^j + g^j = h^j$, then we have a proof of FLT, because this counterexample is smaller than the minimum counterexample, a contradiction.

To pursue our thinking further: let m be an appropriate modulus. Assume $a + b = c$. Then for all i, j, k such that $i + j = k$, $(a - im) + (b - jm) = (c - km)$. So there is an infinity of equalities among the triples $<d, e, f>$ that are congruent to $<a, b, c>$, respectively. Hence there is an infinity of equalities among the triples $<d, e, f>$ that are congruent to $<x^p, y^p, z^p)$, respectively.

Our next endeavor should probably be to find out more details about the relationship between x^j and x^p, y^j and y^p, and z^j and z^p, when $j \equiv p \bmod q - 1$.

Third Approach Using Powers of *a*, *b*, *c*

3rd Condition for Truth of FLT

If there exists a prime q such that:
$(x, q) = (y, q) = (z, q) = 1$, and
and $a \equiv x$, $b \equiv y$, and $c \equiv z \bmod q$, and
$a^p + b^p < q$ and $c^p < q$,
Then FLT is true.

Proof:

We have a contradiction that implies the truth of FLT. For, on the one hand, $a^p \equiv x^p$, $b^p \equiv y^p$, $c^p \equiv z^p \bmod q$ by a basic fact of congruence theory. So $a^p + b^p \equiv c^p \bmod q$. But on the other hand $a^p + b^p$ not $\equiv c^p \bmod q$ because $a^p + b^p \neq$ to c^p (the contrary would imply a minimum counterxample smaller than the minimum counterexample), and $a^p + b^p < q$, and $c^p < q$. □

The Condition generalizes to compound moduli m via Euler's Totient Function, $\varphi(m)$.

Discussion of the 3rd Condition for Truth of FLT

We must confess that we have become rather pessimistic about the possibility of a proof of FLT via the 3rd Condition. The reason is that the range of moduli q is very limited — namely, to q such that x, y, z are greater than q, so that minimum residues a, b, c, exist that are congruent to, and different from, x, y, z respectively, mod q, and furthermore are small enough such that $a^p + b^p < q$ and $c^p < q$.

If q is large enough that x, y, z are each less than q, then there are no such a, b, c, and it appears that we can do nothing.

A Fundamental Difficulty in Proving FLT Via These Approaches

If $e + f < m$ and $g < m$, for some prime modulus q, call $e + f - g$ a *bottom element* of the set of e', f', g' that are congruent to e, f, g respectively, call that set of elements a *stack*.

No stack having a bottom element $a^1 + b^1 - c^1 = 0$ can contain a counterexample (Lemma 0.0, Part (1) of this paper, on occampress.com), and no stack having a bottom element $a^2 + b^2 - c^2 = 0$ can contain a counterexample (Lemma 0.5, Part (1) of this paper, on occampress.com), and no stack having a bottom element $a^k + b^k - c^k \neq 0$ can contain a counterexample, and so the reader might be tempted to conclude that we have our proof of FLT.

The problem is that the set of bottom elements mod m is in general never the set $S = \{a^1 + b^1 - c^1, a^2 + b^2 - c^2, \ldots, a^{\varphi(m)-1} + b^{\varphi(m)-1} - c^{\varphi(m)-1}\}$, since in general none of $a^{\varphi(m)-1}$, $b^{\varphi(m)-1}$, and $c^{\varphi(m)-1}$ can be less than m. But S is the set that is required to guarantee that a counterexample is in a stack.

The reader might reply that if all the elements of S are not equal to 0, then that forces a contradiction, since the counterexample must be congruent to 0 mod m. But that is incorrect. For, assume $a^k + b^k - c^k$ in $S = mU$. Then $a^k + b^k - c^k \equiv 0 \bmod m$, and thus a counterexample could be an element of the corresponding stack without contradiction. It is only when $a^k + b^k$, hence $a^k + b^k - c^k$, $< m$ that we can be sure that $a^k + b^k - c^k$ not $\equiv 0$, and thus that no counterexample can be contained, without contradiction, in the stack having $a^k + b^k - c^k$ as bottom element.

Our first attempts to overcome the fact that not all required bottom elements could be present in any modulus, were to try to show that an assumed counterexample always had to be in the

stacks having bottom elements with exponents near $\varphi(m) - 1$. We called these attempts the "pushing up" or "pushing away" strategy. In other words, we tried to show that a counterexample $x^p + y^p - z^p$ never became a bottom element, which meant that a counterexample did not exist, since for each positive integer, there is a minimum modulus m such that the integer is less than m. But we were unable to make this strategy work.

At present, our best attempts to overcome this difficulty are described in "Approaches Using Only Powers of x, y, z (Congruent Sets)" on page 19.

Facts amd Observations Regarding $U(p, a, b, c)$

Let $U(p, a, b, c) = a^p + b^p - c^p$, where $a, b, c \geq 1$. Each of the $U(p, a, b, c)$ (except for the case that $a = x$, $b = y$, and $c = z$) are products of primes.

Let m be an appropriate modulus. It too is a product of primes. Let $a = x - im$, $b = y - jm$, $c = z - im$, where here i, j, k are integers, positive or negative, or in no more than two cases, 0 . It follows that $a^p \equiv x^p$, $b^p \equiv y^p$, $c^p \equiv z^p \bmod m$.

We have:

(1)
$U(p, a, b, c) = a^p + b^p - c^p = (x - im)^p + (y - jm)^p - (z - km)^p.$

(1) must equal Rm, where $R \neq 0$. The proof is as follows: We know that $U(p, a, b, c) \equiv (U(p, x, y, z) = 0) \bmod m$. By the binomial theorem we know that the right-hand side of (1) equals $(x^p - Uim) + (y^p - Vjm) - (z^p - Wkm)$. By assumption that $x^p + y^p - z^p = 0$, we get:

$-Uim - Vjm + Wkm = (-Ui - Vj + Wk)m = Rm$ □

We call to the reader's attention the following. Consider $a^p + b^p - c^p = (x - im)^p + (y - jm)^p - (z - km)^p$. For *each r* that is a *common* factor of im, jm, and km, there exists (by what we have said above) an S such that $a^p + b^p - c^p = Sr$, or, in other words, such that $U(p, a, b, c) \equiv 0 \bmod r$. So a given $a^p + b^p - c^p$ can be congruent to 0 mod more than one modulus. This would rarely be the case if a counterexample to FLT did not exist. So, we see that the existence of a counterexample has "consequences" (for further details see ""Consequences" of a Counterexample" on page 54).

Furthermore, each $a^p + b^p - c^p$ is a factor in an infinity of other $a'^p + b'^p - c'^p$. For, let $a^p + b^p - c^p = Rm$. Let $m' = RmU$, and make m' the common factor of im', jm', km' for some $a'^p + b'^p - c'^p$. Then $a'^p + b'^p - c'^p = SRmU$. Or $a'^p + b'^p - c'^p = S(a^p + b^p - c^p)U$. There is a countable infinity of im', jm', km' having Rm as the common factor.

Obviously, we should investigate small m — 2, 3, 4, etc. — and, working with the minimum residues u, v, w that x, y, z must be congruent to respectively, see if we can prove that there is a case where $u^p + v^p - w^p \neq Rm$, a contradiction that would give us a proof of FLT.

Another approach using $U(p, a, b, c)$ might be developed using infinitary matrices ala Cantor, with, say, values of $U(p, a, b, c)$ running vertically (down the left-hand side of the matrix), and moduli running horizontally (across the top of the matrix). A check mark in the cell $[U(p, a, b, c), m]$ would mean that $U(p, a, b, c) \equiv 0 \bmod m$, or, in other words, that $U(p, a, b, c)$ is a multiple of

m.

Simplest Approach Using *U*(*p*, *a*, *b*, *c*)

1. Assume a counterexample $x^p + y^p - z^p = 0$ exists. Now consider:

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

This expression =

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

because the counterexample expression = 0.

Now (1) can be expressed as

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

We now ask if (3) can equal (2). If not, then we have a proof of FLT.

Note: I proved several years ago that if $x^p + y^p - z^p = 0$, then for all k, where $1 \le k < p$, and k here is real, not merely an integer, $x^k + y^k - z^k > 0$.

Remarks

(A) A naive person might argue that (3) = (2) if $x - 1 = -1$, $y - 1 = -1$, and $z - 1 = -1$. But these equations imply $x = y = z = 0$, which is false. And so therefore (3) ≠ (2) and we have our proof of FLT.

The trouble is that we have not shown that the three equalities we have just stated, are the *only* way that (3) can equal (2).

(B) By *Note*, (2) is negative. A plausibility argument that (3) is positive is that, since x, y, z were known, prior to Wiles' proof, to be very large numbers, $x^{(p-1)}(x-1)$ is very slightly less than x^p, $y^{(p-1)}(y-1)$ is very slightly less than y^p and $z^{(p-1)}(z-1)$ is very slightly less than z^p. Therefore (3) is positive. If this is true, then we have a contradiction that gives us a proof of FLT.

One problem here is that our proof of several years ago deals only with continuous various in k, not with continuous variations in x, y, z.

.

Approaches Using Only Powers of *x*, *y*, *z* (Congruent Sets)

Definition of "Congruent Set"

Definition of "$U(k, x, y, z)$"

For $x. y, z$, constituents of an assumed counterexample $x^p + y^p = z^p$, and for each $k \geq 1$, $U(k, x, y, z)$ denotes $x^k + y^k - z^k$.

We remark in passing that each $U(k, x, y, z)$ is a point on the curve $f(k) = x^k + y^k - z^k$ as defined in the section "First Vertical Approach Using the Calculus" in Part (1) of this paper, on occam-press.com.

Statement (A)

Let q be an odd prime. Then the following sets of congruent $U(k, x, y, z)$ exist. We call each such set a *congruent set mod q*, or, if q is understood, then simply a *congruent set*.

$\{U(k, x, y, z) \mid k \equiv 1 \bmod q - 1\}$,
$\{U(k, x, y, z) \mid k \equiv 2 \bmod q - 1\}$,
...
$\{U(k, x, y, z) \mid k \equiv q - 1 \bmod q - 1\}$,

Proof of Statement (A)

(**Step A.1**)
If q is an odd prime and u is a positive integer, then $u^r \equiv u^{r + j(q-1)} \bmod q$, where $r \geq 1, j \geq 0$.
Proof of step (A.1):
There are two cases: (I) $(u, q) = 1$ and (II) $(u, q) \neq 1$.

Case I:
By Fermat's Little Theorem, we know that $1 \equiv u^{q-1} \bmod q$. The result follows by repeated multiplying of both sides of the congruence by u. □

Case II:
If u and q have a factor in common, that factor must be q. Therefore, by definition of the integers mod q, u is congruent to all multiples of q. Thus, in particular, $u^1 \equiv u^{1+q-1} \bmod q$, The result follows by repeated multiplying both sides of the congruence by u. □

(**Step A.2**)
It follows from (Step A.1) that

$$x^i \equiv x^{i + j(q-1)} mod \ \ q$$

$$y^i \equiv y^{i + j(q-1)} mod \ \ q$$

$$z^i \equiv z^{i+j(q-1)} mod\ \ q$$

where $j \geq 0$, and $1 \leq i \leq q-1$. Therefore, by a basic fact of congruence theory, $U(i, x, y, z) \equiv U(i + j(q-1), x, y, z)$. □

We call $U(i, x, y, z)$, where $1 \leq i \leq q-1$, the *base element* of its congruent set. But this does not mean that $U(i, x, y, z)$ lies on the zero-level in our lines-and-circles model of congruence. The successive values of the $U(i, x, y, z)$ can "jump around": some may be positive, some negative, one may be zero. The term base element refers only to the location of $U(i, x, y, z)$ relative to other $U(k, x, y, z)$.

We call the set $\{U(i + j(q-1), x, y, z)\}$, where $1 \leq i \leq q-1$ and j is constant, a *row* in the set of all congruent sets mod q.

The set of congruent sets mod q is the same, regardless if a counterexample exists or not. Thus, regardless if a counterexample exists or not, for $q < p$, the element $U(p, x, y, z)$ is *not* a base element even though its value is 0. For all $q \geq p$, $U(p, x, y, z)$ *is* a base element.

Since, if a counterexample exists, $U(p, x, y, z) \equiv 0 \bmod q$, it follows that all elements in the congruent set containing $U(p, x, y, z)$ — whether or not $U(p, x, y, z)$ is the base element — are likewise congruent to 0 mod q — that is, are multiples of q. Hence the base element cannot be relatively prime to q.

We emphasize that ongruent sets merely establish *congruences* between $U(k, x, y, z)$ mod q. Congruent sets do not determine the *values* of the $U(k, x, y, z)$, because to say that $u \equiv v \bmod m$ is to say only that u and v differ by some multiple of m. It is not to say what the actual values of u and v are. Thus the *values* of the $U(k, x, y, z)$ in a given congruent set are all congruent, hence are all elements of one congruence class mod q, but they are in general not in the same *order* (increasing order) as the elements of a congruence class normally are.

Basic Facts About $U(k, x, y, z)$ And Congruent Sets

- There is a countable infinity of $U(k, x, y, z)$.
- The value of each $U(k, x, y, z)$ is fixed.
- For each modulus q, $U(k, x, y, z)$ is an element of exactly one of the above congruent sets.
- For *each* modulus q, there are $q-1$ congruent sets, but q congruence classes mod q.
- If $k = p + j\,(q-1)$ — that is, if $U(k, x, y, z)$ is congruent to 0 mod q and q is odd, then k is odd. (Follows directly from the fact that p is odd and that for all $q > 2$, $(q-1)$ is even.)
- $U(0, x, y, z) = 1$ because $x^0 + y^0 - z^0 = 1$.

$U(1, x, y, z) = Kdef$, where $K \geq 1$, and $d, e, f > 1$; $Kdef$ contains the factors 2 and p, d is a factor of x, e is a factor of y, f is a factor of z, $(d, e, f) = 1$ (Lemma 0.2 in Part (1) of this paper,

on occampress.com). Thus $U(1, x, y, z)$ is a multiple of $2 \cdot 3 \cdot 5 \cdot p$.

$U(k + 1, x, y, z) > U(k, x, y, z)$ for all $k + 1$ such that $0 \le k + 1 \le p - 1$. (Lemma 1.5 in Part (1) of this paper, on occampress.com)

For all $k > p$, $U(k, x, y, z)$ *is negative* (Lemma 1.95 in Part (1) of this paper, on occampress.com).

$U(k + 1, x, y, z) < U(k, x, y, z)$ for all k such that $k > p$. (Lemma 1.5 in Part (1) of this paper, on occampress.com). In other words, the absolute value of $U(k, x, y, z)$ is monotonically increasing, for all $k \ge 1$, except for $k = p$.

Thus, no two $U(k, x, y, z)$ are equal, where $k \ge 1$.

Of course, by assumption, $U(p, x, y, z) = 0$.

• If no counterexample exists, there are two possibilities: (A) The set of prime factors in the values of all $U(k, x, y, z)$ is the set of all primes; (B) The set of prime factors in these values is not the set of all primes.

If a counterexample exists, then there is only one possibility, namely (A). The reason is that if $U(p, x, y, z) = 0$, then for each prime modulus q, there is a congruent set — namely, the one containing $U(p, x, y, z) = 0$ — each of whose members $U(k, x, y, z)$ (except for $U(p, x, y, z)$) is a multiple of q.

In fact, as we will see below under "First Version of Approach: Show a U(k, x, y, z) Has Two Different Values" on page 29, if a counterexample exists, then for each finite set of primes, there is an infinity of $U(k, x, y, z)$ that are multiples of the product of the elements of that set.

Definition of "Location" of $U(k, x, y, z)$

• (2)

For each prime modulus q, each $U(k, x, y, z)$ — including $U(p, x, y, z)$ — has a *location* in the set of congruent sets mod q. A *location* is defined by the ordered pair (i, *row*), where i is the exponent of the base element of a congruent set — thus $1 \le i \le q - 1$ — and *row* is the value of j in $k = i + j(q - 1)$, where $j \ge 0$. In other words, i is the remainder of $k/(q - 1)$, and *row* is the quotient of $k/(q - 1)$. A congruent set mod q is therefore the set of all $U(k, x, y, z)$ such that, for some i, where $1 \le i \le q - 1$, $k \equiv i \bmod (q - 1)$.

The location of $U(k, x, y, z)$ is the same whether or not a counterexample exists. Even though the *value* of a $U(k, x, y, z)$ may differ, depending on whether a counterexample exists or not, the *location* of $U(k, x, y, z)$ does not differ.

• Membership in a congruent set is solely a function of k, not of the value of $U(k, x, y, z)$. Each $U(k, x, y, z)$ — including $U(p, x, y, z)$ — is an element of one and only one congruent set. Since $U(p, x, y, z) \equiv 0 \bmod q$, it follows that all elements in the congruent set containing $U(p, x, y, z)$ are likewise congruent to 0 mod q — that is, are multiples of q. This is true regardless of the location (i, *level*) of $U(p, x, y, z)$ in the congruent set.

Congruent *Sets* vs. Congruence *Classes*

• It is possible for the elements of two or more congruent *sets* mod q to be in the same congruence *class* mod q, but it is not possible for the elements of one congruent *set* to be in two or more different congruence *classes* mod q. (Follows from the fact that all members of a congruent set are congruent mod q.)

Congruent Sets Containing $U(p, x, y, z) = 0$

• $U(p, x, y, z)$ cannot be an element of a congruent set whose base element has an *even* exponent k. The reason is that, since $(q - 1)$ is always even, the exponent $k + j(q - 1)$, where k is even, must be even. But p is odd. However, if k is odd, as is the case for the exponent p, $k + j(q - 1)$ is odd.

Values of all $U(k, x, y, z)$

• The *values* of all $U(k, x, y, z)$ in a congruent set mod q are congruent mod q. In more detail:

• (1)

If q is prime, then if $k \equiv k'$ mod $(q - 1)$ then $U(k, x, y, z) \equiv U(k', x, y, z)$ mod q, hence $U(k, x, y, z)$ and $U(k', x, y, z)$ are in the same congruent set mod q.

Proof: Follows from Fermat's Little Theorem, and the definition of *congruent set.*

• (1.5)

$a^k \equiv a^{k'}$ mod $(q - 1)$ iff $k \equiv k'$ mod $\varphi(q - 1)$. Thus $U(k, x, y, z) \equiv U(k', x, y, z)$ mod $(q - 1)$ iff $k \equiv k'$ mod $\varphi(q - 1)$.

Proof: Follows from Eurler's generalization of Fermat's Little Theorem, and the definition of *congruent set.*

(I am indebted to a graduate student for bringing statement (1.5) to my attention.)

Thus (from (1)), the congruent set mod q with base element $U(i, x, y, z)$, where $1 \le i \le q - 1$, is the set $U(k, x, y, z)$ such that $k \equiv i$ mod $(q - 1)$. No congruent set is defined by the values of the $U(k, x, y, z)$ in each set. However, by Fermat's Little Theorem, the values of all the $U(k, x, y, z)$ in a given congruent set are congruent mod q.

The values of no two $U(k, x, y, z)$ are the same (Lemmas 1.5 and 1.95 in Part (1) of "Is There a 'Simple' Proof of Fermat's Last Theorem?", on occampress.com).

• For all $k + 1$, where $1 \le k + 1 \le p - 1$, $U(k + 1, x, y, z) > U(k, x, y, z)$ (Lemma 1.5 in Part (2) of this paper, on occampress.com)

For all $k > p$, $U(k, x, y, z)$ is negative and $U(k + 1, x, y, z) < U(k, x, y, z)$ (Lemma 1.5 in Part (2) of this paper, on occampress.com).

• Each $U(k, x, y, z)$, where $k \ge 1$, is eventually — that is, for some smallest prime modulus q — a base element of a congruent set, and is a base element of a congruent set for all larger moduli. (This is the "touching-down" phenomenon that is described in "Definition of "Touches Down"" on page 12.)

Values of $U(k, x, y, z)$, k Odd

• The value of $U(1, x, y, z)$ is a proper multiple of $2 \cdot 3 \cdot 5 \cdot p$ (Lemma 0.2 in Part (2) of this

paper, on occampress.com).

- Each $U(k, x, y, z)$, where $k \geq 1$ and odd and not equal to 0, is a multiple of 3. (See "Fact About the Factor (3 – 1)" on page 30.)

Distribution of $U(k, x, y, z)$ As a Function of Prime Factors of k

- Consider any modulus $q > p$, and the associated congruent set for p, namely, $\{U(k_p, x, y, z) \mid U(k_p, x, y, z) \equiv U(p, x, y, z) \bmod q - 1\}$ The elements of this set are the set of all $U(k, x, y, z)$ such that $k = p + j(q - 1)$, where j is a positive integer. Each such $U(k, x, y, z)$ is a multiple of q, because each such $U(k, x, y, z)$ is congruent to 0 mod q.

Now let $J = \{q_1, q_2, ..., q_n\}$ be any finite set of prime moduli. Then, since j is any positive integer, there exists a j that has factors $(q_1 - 1), (q_2 - 1), ..., (q_n - 1)$. This means that $U(p + j(q - 1), x, y, z)$ must equal $wq_1q_2...q_n$, where $w \geq 1$. The reason is that for each i, where $1 \leq i \leq n$, $p + j(q - 1) = p + v(q - 1)(q_i - 1)$, so that $U(p + j(q - 1), x, y, z) = U(p + v(q - 1)(q_i - 1), x, y, z)$ is an element of the congruent set $\{U(k_p, x, y, z) \mid U(k_p, x, y, z) \equiv U(p, x, y, z) = 0 \bmod q_i\}$.

It follows that for each finite product of primes, there exists an infinity of U each of which is a multiple of that product.

Can this fact be used to arrive at a contradiction, since for each modulus q, there are q congruence classes, but only $q - 1$ congruent sets? (A congruence class is "missing" from the set of congruent sets.) Thus there is a countable infinity of countable infinities of values that are excluded for any U. And yet, to repeat: for each finite product of primes, there exists an infinity of U each of which is a multiple of that product. The problem is that we do not know what *other* prime factors are in the value of each U. They may be such as to exclude U from the "missing" congruence classes, and thus deprive us of a contradiction.

- If q is a prime appropriate modulus, consider the infinite sequence of appropriate moduli, q^1, q^2, q^3, ... We have the following, by assumption of a counterexample:

a countable infinity Q_1 of $U(k, x, y, z)$ are multiples of q^1;
a countable infinity Q_2 of $U(k, x, y, z)$ are multiples of q^2; $Q_2 \subseteq Q_1$;
a countable infinity Q_3 of $U(k, x, y, z)$ are multiples of q^3, $Q_3 \subseteq Q_2$;
...

(The reason for these statements is that, e.g., $mq^3 = (mq)q^2$, and thus mq^3 is a multiple of q^2.)

Since there is an infinity of such q (because there are only a finite number of different prime factors in x, y, and z), there is a countable infinity of countable infinities of $U(k, x, y, z)$ that are multiples of powers of primes. Indeed, the same holds for all appropriate moduli. But, as is well-known, a countable infinity of countable infinities is still only a countable infinity, so there is no immediate contradiction here.

Facts and Observations Regarding Possibility of Showing a $U(k, x, y, z)$ Has More Than One Value

- It is impossible for $U(p + j(q - 1), x, y, z)$ to have two or more values by definition, since $U(p + j(q - 1), x, y, z) = x^{p + j(q-1)} + y^{p + j(q-1)} - z^{p + j(q-1)}$.

In "First Version of Approach: Show a U(k, x, y, z) Has Two Different Values" on page 29 we attempt to show that since it is possible for a factor $(q_i - 1)$ in j to have a divisor $(q_h - 1)$, it is possible for $U(p + j(q - 1), x, y, z)$ to have two values, a contradiction. We do not deal with the possibility that not only might $(q_i - 1)$ in j have a divisor $(q_h - 1)$, but that $(q_r - 1)$ might also have a divisor $(q_s' - 1)$, and so on for a finite succession of divisors of similar divisors. At present we believe that this fact might lead to further contradictions that would give us a proof of FLT.

We should keep in mind the following:

(1)

Let q be a prime modulus. Then:

(a) For each $n \geq 1$, there exists an *infinity* of $U(p + (q - 1)(q_1 - 1)(q_2 - 1) \ldots (q_n - 1), x, y, z)$, where q_i is a prime modulus, that are elements of the congruent set mod q having $U(p, x, y, z)$ as base element. Furthermore,

(b) For *each* such product $(q_1 - 1)(q_2 - 1) \ldots (q_n - 1)$, there is an *infinity* of U in the same congruent set having the product $(q_1 - 1)(q_2 - 1) \ldots (q_n - 1)$ in its exponent.

Proof of (a):

Follows from "Statement (A)" on page 20, and from the fact that there is a countable infinity of prime moduli since each prime greater than the largest prime in x, y, and z is a prime modulus. □

Proof of (b):

For each $r \geq 1$, $p + r(q - 1)(q_1 - 1)(q_2 - 1) \ldots (q_n - 1)$ is the exponent of a U in the congruent set having $U(p, x, y, z)$ as its base element. □

Furthermore, as stated in "Proof of Statement (A)" on page 20, each U having $(q - 1)(q_1 - 1)(q_2 - 1) \ldots (q_n - 1)$ in its exponent is an element of the congruent set having $U(p, x, y, z)$ as its base element *for each prime modulus* q_i, where $1 \leq i \leq n$.

Do these facts imply that there are "too many" exponents? For a given prime modulus q, let us consider the set of congruent sets mod q having $U(p, x, y, z)$ as base element. Ignoring negative j for the moment, the exponents of the U in this set are

$p + (1)(q - 1)$,
$p + (2)(q - 1)$,
$p + (3)(q - 1)$,
...

A countable infinity of elements. But now from (1) we know that $(q - 1)$ for each of (1), (2), (3), ... is the root of an infinitary tree, because each $(q - 1)$ can be immediately followed by one of a countable infinity of $(q_i - 1)$. That is, for *each* prime modulus q_i there exists:

an exponent $p + (1)(q - 1)(q_i - 1)$,
an exponent $p + (2)(q - 1)(q_i - 1)$,
an exponent $p + (3)(q - 1)(q_i - 1)$,
...

for an infinity of q_i. But then, similarly, each $(q_i - 1)$ can be immediately followed by one of a countable infinity of $(q_i' - 1)$. And so on. Which gives us an infinity tree of infinite depth.

Do we have the makings of a conflict in cardinalities? We recall that the number of infinite *paths* in an infinitely deep binary tree is uncountable. But it is straightforward to show that there is only a countable infinity of *nodes* in an infinitely deep infinitary tree:

Let the root of the tree have branches to the initial $(q - 1)$s in the above exponents. Number the branches from each node 1, 2, 3, ... and let each node be identified by the path leading to it, with a comma separating the branches. Thus, for example, a third level node is identified by the path 1, 539, 76.

Now list all paths in order of increasing number of digits, counting the comma as a digit. First comes the (finite) list of paths of length one, then the (finite) list of paths of length two, then the (finite) list of paths of length three, etc.

It is clear that the paths can be numbered 1, 2, 3, 4, ... and therefore that the paths, hence the nodes, can be matched one-one with the positive integers, and so the number of nodes in the infinitary tree is countably infinite.

However, by (1)(b), we know that for *each node*, there is a *countable infinity* of exponents containing the same product $(q - 1)(q_1 - 1)(q_2 - 1) \ldots (q_n - 1)$. Unfortunately, the total number of exponents remains only countably infinite, via the rule expressed informally as "a countable infinity of countable infinities is a countable infinity". Specifically, we can extend from each node the countable infinity of exponents containing the same product that is represented by the node (the order of the exponents doesn't matter), and then use the diagonal argument that Cantor used to show that the cardinality of the rational fractions is the same as the cardinality of the integers.

The reader may wonder about repetitions of $(q_i - 1)$ terms in a given exponent. Unfortunately, this possibility, too, does not obviously give us a contradiction via incompatible cardinalities. For, in our representation of nodes in the infinitary tree described above, we can simply use, say, hyphens to separate repetitions of a $(q_i - 1)$ term. Thus in our example of the specification of a node, that is, 1, 539, 76, if the last term in the node were repeated three times, then we would write, 1, 539, 76-76-76, ... It is clear that our ordering of node paths by length of specification is not affected by this modification in node specification.

Other facts and observations:

• Without loss of generality, we can stipulate that all products $(q_1 - 1)(q_2 - 1) \ldots (q_n - 1)$ in an exponent be written in non-decreasing order of q_i (we say "non-decreasing" to allow for multiple occurrences of a given $q_i - 1$) term).

• For fixed $q, q_1, q_2, \ldots, q_n$, where $n \geq 0$, an easy way to specify a countable infinity of expo-

nents $p + v(q-1)(q_1-1)(q_2-1) \ldots (q_n-1)$ such that v contains no (q_r-1) term is simply to let the set of v be the set of odd, positive integers. This works because all q_r are odd primes., hence all (q_r-1) terms are even.

• Consider the infinite set of exponents $p + v(q-1)$. The corresponding values of $U(p + v(q-1), x, y, z)$ are wq, $w'q$, $w''q$, ... , where the values are monotonically decreasing (Lemma 1.5 in Part (1) of this paper, on occampress.com). The same applies for all products $(q-1)(q_1-1)(q_2-1) \ldots (q_n-1)$.

• If q_1 is an odd prime, then there exists a prime q such that $(q-1) = w(q_1-1)$.

Proof:

Let S denote the set of integers modulo (q_1-1). Then by Dirichlet's celebrated theorem, there exists an infinity of primes in the congruence class whose minimum residue is 1 — that is, in the set $\{1 + u(q_1-1)\}$. Let q be any such prime that is greater than q_1. Then $(q-1)$ is an element of the congruence class whose minimum residue is 0 — that is, the congruence class containing all multiples of (q_1-1). Thus $(q-1) = w(q_1-1)$. □

Facts and Observations Regarding Possibility of Showing Two $U(k, x, y, z)$ Have the Same Value

It is impossible for two or more $U(p + j(q-1), x, y, z)$ to have the same value because $U(k+1, x, y, z) < U(k, x, y, z)$ for all $k > p$. (Lemma 1.5 in Part (1) of this paper, on occampress.com) We remark in passing that for all $k > p$, $U(k, x, y, z)$ *is negative* (Lemma 1.95 in Part (1) of this paper, on occampress.com).

• A tempting Approach is the following.

All primes larger than the largest prime in x, y, and z are prime moduli.

Suppose, now, that for some prime modulus q there exists $U(p + j(q-1), x, y, z) = wq$. where w is a product of primes each of which is a prime modulus.

Suppose, further, that for one of the primes q' in w we have $U(p + j(q'-1), x, y, z) = w'q' = wq$. Then $U(p + j(q-1), x, y, z)$ and $U(p + j(q'-1), x, y, z)$ have the same value, and we have a contradiction that gives us a proof of FLT.

However, we must remind the reader that in the case of Possibility (1), we have full control over the value of j in the exponent $p + j(q-1)$, whereas in the present case, we have no way of controlling the value of w in the value wq of $U(p + j(q-1), x, y, z)$. Thus at present we believe that Possibility (1) offers the most promising Approach to a proof of FLT.

Another consideration:

• Suppose that in the mod q congruent set having $U(p, x, y, z)$ as base element, we consider the exponent $p + v(q-1)(q_1-1)$, where v is here a fixed value. Then $U(p + v(q-1)(q_1-1), x, y, z) = wqq_1$. Now in the mod q_1 congruent set having $U(p, x, y, z)$ as base element, consider the exponent $p + v(q_1-1)(q-1)$, where v is the same value as before. Is it necessarily true that $U(p + v(q_1-1)(q-1), x, y, z) = wqq_1$?

Facts and Observations Regarding the Set of all Congruent Sets

It is clear, from basic facts of congruences, that for each modulus q each $U(k, x, y, z)$, where $k \geq 1$, is an element of one congruent set mod q. Furthermore, it is clear how the k in each component set are related (they are congruent mod $q - 1$ to the exponent of the base element of the set).

We now ask how the values of the $U(k, x, y, z)$ in each congruent set are related. We know only that the values are congruent mod q, and that the absolute value of each $U(k, x, y, z)$ must be greater than that of its predecessor (Lemma 1.5 in Part (1) of this paper, on occampress.com).

We observe in passing that, for each modulus q, there are elements of congruent sets that are the same regardless if a counterexample to FLT exists are not. For example, this is true of $(x^3 + y^3 - z^3)$. (Remember that x, y, z are fixed elements of an assumed counterexample, and that FLT had been proved true for the exponent 3 more than a century prior to Wiles' proof of FLT for all exponents. In other words, more than a century prior to Wiles' proof, it was known that for all positive integers a, b, c, $a^3 + b^3 - c^3$ was not equal to zero.)

The fact that some $U(k,$

Checklist to Avoid Futile Approaches

We have found that a great deal of useless effort can be avoided if, at the beginning of work on an approach to a proof of FLT, we ask two questions:

(1) How does the phenomenon on which this approach is based, appear if a counterexample does not exist?

(2) Is the approach based on the possibility of a $U(k, x, y, z)$ being in the wrong location in a congruent set mod q? If the approach is based on the possibility of a wrong location, then it is probably not worth pursuing, because, for each q, each $U(k, x, y, z)$ has exactly one location in a congruent set mod q regardless if a counterexample exists or not. (See "Definition of "Location" of U(k, x, y, z)" on page 22.)

In some of the approaches that follow, it will be clear that we did not first ask these two questions. The reader should be appropriately skeptical regarding these approaches.

Approach: Show There is a *q* Such That *U*(*p*, *x*, *y*, *z*) Is Not In Any Congruent Set Mod *q*

We will have a proof of FLT if we can show that there exists a prime q such that

(1)
$(U(1, x, y, z), q) = (U(2, x, y, z), q) = \ldots = (U(q - 1), x, y, z), q) = 1.$

The reason we will have a proof is the following. Clearly, (1) implies that no base element $U(i, x, y, z)$ of a congruent set is a multiple of q. If it were, then $(U(i, x, y, z), q)$ would equal q, contrary to (1). Therefore no element of any of the congruent sets is a multiple of q. But since $U(p, x, y, z) = 0$, it follows that *all* elements of one congruent set must be multiples of q. This contradiction gives us our proof of FLT.

It is clear from (1) that $q - 1$ must be less than p. Otherwise, $U(p, x, y, z)$ would be a base ele-

ment and since $(0, q) \neq 1$, condition (1) would not hold.

Approach: Show Contradiction in Elements of the $U(p, x, y, z)$ Congruent Set

First Version of Approach: Show a $U(k, x, y, z)$ Has Two Different Values

1. Let q be a prime modulus, and consider the mod q congruent set for the exponent p, namely, $\{U(k, x, y, z) \mid k \equiv p \mod q - 1\}$. The elements of this set are the set of all $U(k, x, y, z)$ such that $k = p + j(q - 1)$, where j is *any* non-negative integer. Each such $U(k, x, y, z)$ is a multiple of q, because each such $U(k, x, y, z)$ is congruent to 0 mod q.

2. Now consider the set of all $k = p + j(q - 1)$.

We can choose any integer j we like — that is, we can choose any factors we like for j. So we can choose $j = v(q_1 - 1)(q_2 - 1) \ldots (q_n - 1)$, where:

n may be 0, and
it is possible that some terms are repetitions of other terms, and
q and all the q_i's are odd primes, and
v is an integer.

(1)
It then follows that $U((p + v(q_1 - 1)(q_2 - 1) \ldots (q_n - 1)(q - 1)), x, y, z) = wq_1q_2 \ldots q_nq$.

(It is possible that if the term $(q_i - 1)$ is repeated m times, we shall have to write $wq_1q_2 \ldots q_i^m \ldots q_n\, q$, but we temporarily put aside this question.
The value of w cannot be 0 except in the case of the assumed counterexample. See Lemmas 1.5 and 1.95 in Part (1) of this paper, on occampress.com.

Proof of statement (1):
It must be that $U(p + v(q - 1)(q_1 - 1)(q_2 - 1) \ldots (q_n - 1), x, y, z)$ is an element of:

the congruent set mod q having $U(p, x, y, z)$ as base element, *and*
the congruent set mod q_1 having $U(p, x, y, z)$ as base element, *and*
the congruent set mod q_2 having $U(p, x, y, z)$ as base element, *and*
...
the congruent set mod q_n having $U(p, x, y, z)$ as base element.

This can only be if $U(p + v(q_1 - 1)(q_2 - 1) \ldots (q_n - 1)(q - 1), x, y, z) = wq_1q_2 \ldots q_nq$. □

3. In the exponent $k = p + j(q - 1)$, j can be *any* positive integer, and so we can choose primes q_i, q_r, q_h, such that no two of these primes are equal, and such that:

the exponent $k = p + a(q - 1)(q_1 - 1)$,
$a(q_h - 1) = (q_1 - 1)$, where a is an odd prime. (For example, if $a = 3$, $q_h = 13$, then $q_1 = 37$, because $3(13 - 1) = 37 - 1$).

We now claim that $U(k, x, y, z)$ has at least two values.

For, if we write k as $k = p + (q - 1)(q_1 - 1)$, then $U(k, x, y, z) = wqq_1$.
But if we write the same k as $k = p + (q - 1)a(q_h - 1)$, then $U(k, x, y, z) = w'qq_h$.

We claim that the reason these two values of U are different is that w and w' cannot somehow make them equal, since neither w nor w' contains a proper fraction. In more detail, our argument is as follows:

3.1. Assume, to the contrary, that $wqq_1 = w'qq_h$.

3.2. Then it must be that w contains the factor q_h and that w' contains the factor q_1. But then the assumed equal values of U each contain the factor q_hq_r, which implies that the exponent $k = p + a(q - 1)(q_1 - 1)(q_h - 1)$, contrary to our assumption that $k = p + a(q - 1)(q_1 - 1)$.

Another argument is the following: for each q and each j, there are at least two factoring rules of $j(q - 1)$: (1) a factoring utilizing solely terms $(q_i - 1)$ and odd primes, where each $(q_i - 1)$ does not divide a $(q_s - 1)$, and (2) a factoring utilizing solely terms $(q_r - 1)$ where each $(q - 1)$ has no divisors $(q_h - 1)$, and odd primes. Rule (2) will contain all factors $(3 - 1)$ in $j(q - 1)$, whereas Rule (1) will not.

It is clear the value of each U will differ, depending on which factoring is used. But that is impossible. For example, consider the case where $j(q - 1) = 1(q - 1)$, and where we factor according to Rule (2). Then the value of U does not contain a q, implying that U is not an element of the congruent set mod q having $U(p, x, y, z)$ as base element, which is absurd.

Criticism of the Approach

Readers have criticized the Approach on the grounds that the equation $U(p + v(q - 1)(q_1 - 1)(q_2 - 1) \ldots (q_n - 1), x, y, z) = wqq_1q_2 \ldots q_n$ places no restrictions on the factors of w except that they must all be integers. Thus w can contain primes derived from any and all the alternate factorings of $j(q - 1)$ in the general expression for each exponent $p + j(q - 1)$. Thus, there is no way of *excluding* certain factors. All we can say is which factors must be *included*, and these are $q, q_1, q_2, \ldots, q_n$.

Fact About the Factor (3 – 1)

Since each factor $(q - 1)$, $(q_i - 1)$ is even, and since $(3 - 1) = 2$ is such a factor, it follows that the set of all $U(p + j2, x, y, z)$ in the congruent set mod 3 having $U(p, x, y, z)$ as base element, is the set of *all* $U(p + j(q - 1), x, y, z)$ *in all congruent sets mod q having* $U(p, x, y, z)$ *as base element, where q is any odd prime*!

The base elements of the congruent sets mod 3 are $U(1, x, y, z)$ and $U(2, x, y, z)$. There are no others. Now, the exponents of all U in the congruent set having $U(2, x, y, z)$ as base element are even ($2 + j2$ is even), and so the exponents of all U in the congruent set having $U(1, x, y, z)$ as base element, are odd. Therefore $U(p, x, y, z) = 0$ is in the latter congruent set. But then it follows that

the value of every U having an odd exponent is a multiple of 3. Whether this fact can be used to obtain a contradiction, we do not know at present.

Second Version of Approach: Show That a $U(p, x, y, z)$ Congruent Set Element is "Missing"

Note: since the exponent ambiguity that underlies this Version, exists for all congruent sets, not just those having $U(p, x, y, z)$ as base element, we must regard this Version as unpromising until we understand the resolution of the ambiguity.

Let q be an odd prime $> p$, and consider the congruent set mod q having $U(p, x, y, z)$ as base element. By definition of *congruent set*, this means that this congruent set = $\{U(k, x, y, z) \mid k \equiv p \mod (q - 1)$, that is, $k = p + j(q - 1)$, where $j \geq 0\}$.

Since j is any non-negative integer, there exists a j such that $j = (q' - 1)u$, where u is a positive integer and q' is an odd prime $> q$. Thus $U(p + ((q' - 1)u)(q - 1), x, y, z)$ is an element of the congruent set mod q having $U(p, x, y, z)$ as base element and an element of the congruent set mod q' having $U(p, x, y, z)$ as base element. If it happens that $u = (q'' - 1)(q''' - 1) ...$ $(q''''\cdots' - 1)v$, where each $q''''\cdots' > p$, then $U(p + ((q' - 1)(q'' - 1)(q''' - 1) ... (q''''\cdots' - 1)v)(q - 1), x, y, z)$ is an element of:

the congruent set mod q having $U(p, x, y, z)$ as base element;
the congruent set mod q' having $U(p, x, y, z)$ as base element;
the congruent set mod q'' having $U(p, x, y, z)$ as base element;
...
the congruent set mod $q''''\cdots'$ having $U(p, x, y, z)$ as base element.

We assert:

Statement (B)

If $j = (q' - 1)u$, then $U(p + j(q - 1), x, y, z)$ is an element of the congruent set mod q' having $U(p, x, y, z)$ as base element.

Statement (C)

For each prime modulus q, each $U(k, x, y, z)$ — including $U(p, x, y, z)$ — has a unique location in the set of congruent sets mod q.

Proof: See "Definition of "Location" of U(k, x, y, z)" on page 22.

Let us return to the modulus q. In the exponent $p + r(q - 1)2^h$, if r is a product of s different primes t, and $s > h$, and for each t, $2t = (q_t - 1)$, where q_t is prime, then if we ask, "In what congruent sets is the U with the exponent $p + r(q - 1)2^h$?", the answer must be "It depends on how we group the factors of $r(q - 1)2^h$." Or, in other words, "It depends on which t's in r we choose to match with the 2's in 2^h — in one grouping, it may be possible to match a given t with a 2; in other grouping, this may not be possible." We claim that, by statement (B), this answer does not guarantee that U will be in all the congruent sets that it needs to be in. Or, more precisely, the answer implies that U is, and is not, a member of a certain congruent set, which is a contradiction (by statement (C)) that seems to give us a proof of FLT.

The following example should make our reasoning clearer.

Suppose $r = 3 \cdot 5 \cdot 11$. Clearly, 3, 5, 11 are different primes; furthermore, $2 \cdot 3 = (7 - 1)$, $2 \cdot 5 = (11 - 1)$, and $2 \cdot 11 = (23 - 1)$, with 7, 11, 23 being different primes. Suppose $h = 2$ and $q = 17$.

Now we ask, "In which congruent sets having base element $U(p, x, y, z)$ is $U(\ p + r(q-1)2^h, x, y, z) = U(\ p + 165(17-1)2^2, x, y, z)$?"

Our answer is: "It depends on how we group the factors of $r \bullet 2^h = (165)2^2$". If we group them $(2 \bullet 3\ )(2 \bullet 5\ )^*(11\ )$, then U is in the congruent sets mod 7 and 11 having $U(p, x, y, z)$ as base element. It is not in the congruent set mod 23 having $U(p, x, y, z)$ as base element (by statement (B)). If we group them $(2 \bullet 3)(2 \bullet 11)^*(5)$, then U is in the congruent sets mod 7 and 23 having $U(p, x, y, z)$ as base element. It is not in the congruent set mod 11 having $U(p, x, y, z)$ as base element (by statement (B))." But if U has a single exponent (and it does, by definition), then U is either in a given congruent set or it isn't (by statement (C)). Yet we have just seen that the congruent set depends on how we group the factors of U's exponent. (The factors are the same in all groupings in our example, because we are dealing with a single exponent.) But this answer implies that U is, and is not, a member of a certain congruent set, which is a contradiction that seems to give us a proof of FLT. (Observe that this ambiguity would not exist in our example if $h = 3$.)

Important Note: what we have said about the exponent ambiguity in congruent sets whose base element is $U(p, x, y, z)$ also applies to all other congruent sets. However, the ambiguity in those cases is not significant. Each U is in the location that its exponent k establishes for it. The reason why the ambiguity is significant in the of congruent sets whose base element is $U(p, x, y, z)$ is that in these sets, the ambiguity affects which other congruent sets whose base element is $U(p, x, y, z)$ the U with the ambiguous k is an element of. That in turn affects the value of U.

In passing, we point out that we have shown in our example that the primes t exist. (These are called *Germain primes*.) Here are a few more:

$t = 23$, because $2(23) = (47 - 1)$,
$t = 29$, because $2(29) = (59 - 1)$,
$t = 41$, because $2(41) = (83 - 1)$,
$t = 43$, because $2(43) = (87 - 1)$,
$t = 53$, because $2(53) = (107 - 1)$,
$t = 89$, because $2(89) = (179 - 1)$,
$t = 113$, because $2(113) = (127 - 1)$.

A finite number suffices for our argument. It is an unsolved problem in number theory whether there are an infinite number of such primes.

Third Version of Approach: Show That a $U(p, x, y, z)$ Congruent Set Element is "Missing"

A related approach is the following. Consider the exponent $k = p + (q' - 1)(q - 1)$ of a U that is an element of the congruent set mod q having $U(p, x, y, z) = 0$ as base element. Suppose that $(q' - 1) = q''(q''' - 1)$, where q', q'' and q''' are unequal odd primes. Such q' exist: $q' = 23$ is an example, for $(23 - 1) = 11(3 - 1)$. We ask what congruent sets having $U(p, x, y, z) = 0$ as base element, U is an element of. One answer is the congruent sets mod q and q' but not mod q'' or q'''. But another answer is the congruent sets mod q and q''' but not q' or q''. Yet U either is in a congruent set or it is not. This contradiction would give us a proof of FLT.

Some readers have argued that, because $(q' - 1) = q''(q''' - 1)$, U is in *both* the congruent set mod q' and in the congruent set mod q'''. However, we question this, because $(q' - 1) \neq$

$(q' - 1)\, q''(q''' - 1)$.

Criticism of This Version

The same apparent contradiction applies if a counterexample does not exist. For then we have the value of $U(p, x, y, z)$ being a finite product of primes, and therefore $U(p, x, y, z)$ is an element of a congruent set mod q whose base element is not $U(p, x, y, z) = 0$. And yet everything we have said about the exponent $k = p + (q' - 1)(q - 1)$ also applies in this case, since the exponent can exist whether or not U is the base element in its congruent set or not.

Approach: Compare $U(k, x, y, z)$'s if a Counterexample Exists/Does Not Exist

We begin by recalling how the location [*line*, *level*] mod q of the *value* of $U(k, x, y, z)$ is determined. (See proof of statement (2) under "Basic Facts About U(k, x, y, z) And Congruent Sets" on page 21.) We simply divide *the value* of $U(k, x, y, z)$ by q. The remainder is *line* (the number of the line in the lines and circles model of congruence (see "Definition of "Lines-and-Circles" Model of Congruence" on page 10), and the quotient is the *level* on that line.

The location is solely a function of the value of $U(k, x, y, z)$. Since the value of each $U(k, x, y, z)$ is a product of primes — possibly the value is only one prime — we know that, for each prime q in the product, $U(k, x, y, z)$ is in a congruent set mod q all of whose members are multiples of q.

If no counterexample exists, there are two possibilities: (A) The set of primes in the values of all $U(k, x, y, z)$ is the set of all primes; (B) The set of primes in these values is not the set of all primes.

If a counterexample exists, then there is only one possibility, namely (A). The reason is that if $U(p, x, y, z) = 0$, then for each prime modulus q, there is a congruent set — namely, the one whose base element is $U(p, x, y, z) = 0$ — each of whose members $U(k, x, y, z)$ (except for $U(p, x, y, z)$) is a multiple of q.

We now ask how exactly we could "get to" the counterexample case, beginning with the no-counterexample case. One way would be by choosing a prime exponent p, and then instead of $U(p, x, y, z)$ having as value the product of only a finite number of primes, we could let $U(p, x, y, z)$ have as value the product of *all* primes. Such a value would be equivalent to $U(p, x, y, z)$ having the value 0. But no integer can be the product of all primes, since there is an infinity of primes. So we conclude that no $U(p, x, y, z)$ can have the value 0 and hence that a counterexample to FLT does not exist.

Error In This Approach

The equation $U(p, x, y, z) = 0$ is not the "limit" of an infinite sequence of increasingly-long products of primes. All we can say is that this equation implies that for any arbitrarily large finite set Q of primes, there exists an infinity of $U((p + \mathbf{j}(q - 1)), x, y, z)$ each of which is a multiple of the primes in Q. The reason is that for each q, there exists an infinity of j each of which is a multiple of all $(q' - 1)$ such that q' is an element of Q. This means that for each q', the infinite set of resulting U is a subset of the set of all $U((p + j(q' - 1)), x, y, z)$ — the congruence set mod q' having $U(p, x, y, z) = 0$ as base element. Each element of this set is a multiple of q'.

Approach Via Fixed-Set

The Concept at the Heart of This Approach

The heart of our Approach is the fact that a counterexample "has consequences". The briefest explanation we can give of what this means is the following: let S be a 4-dimensional space in which each point (r, a, b, c), where r, a, b, c are positive integers, is associated with the value $U(r, a, b, c) = a^r + b^r - c^r$. If $h = (r, a, b, c)$ is a point in S, an *adjacent point* is one in which just one coordinate differs from the corresponding coordinate of h, and then only by ± 1.

It should be immediately clear that the value associated with each point adjacent to a point h, is related to the value in h by virtue of the fact that the same function governs the value of each point in S. So, in particular, if the value associated with a point h is 0 (which would be the case if a counterexample to FLT existed and the coordinates of h were (p, x, y, z)), then the values associated with adjacent points will differ from what they would be if the value in h were not 0. This is an example of what we mean when we say that a counterexample "has consequences".

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

However, if the values associated with adjacent points are known to be the same regardless if a counterexample exists or not (that is, they are elements of the Fixed-Set), then our only conclusion can be that we have a contradiction, because on the one hand, these values are the same, but on the other, they are changed, depending on the existence or non-existence of a counterexample.

For related reading, see the section ""Consequences" of a Counterexample" on page 54 and also the section "Four-Dimensional Approach" in Part (1) of this paper, on the web site occampress.com. The latter section discusses the possibility of "crooked induction" from the point that contains an assumed counterexample.

A Word Regarding a Certain Type of Objection to This Approach

Our Approach is based on a *comparison* between the two cases, a counterexample to FLT exists, and a counterexample to FLT does not exist. A few readers in the past have claimed that this Approach is illegitimate because to compare two mutually exclusive cases is to imply that they both exist simultaneously, which, of course, would not be possible. Our reply to this criticism is that equivalents of such comparisons are made every day. For example:

"If the *abc*-conjecture is true, then ... but if it is false, then ..."

"If an odd, perfect number exists, then ... but if an odd, perfect number does not exist, then..." or,

"If a counterexample to the $3x + 1$ Conjecture exists that results from an infinitely-repeating cycle of odd, positive integers, then there is a computer program that, in principle, will find the counterexample and halt. But if the counterexample is not part of an infinitely-repeating cycle, then the program will run forever," or,

(Prior to the confirmation of the existence of the Higgs boson), "If the Higgs boson exists, then ... but if it doesn't exist, then ..."

Furthermore, a simple truth-table argument shows that the readers' claim is false. Let p

denote "Counterexamples to Conjecture *X* exist". Now consider:

(1)
$(p \Rightarrow r)$ and $(\sim p \Rightarrow s) \Rightarrow (p$ and $\sim p)$,

where "⇒" denotes "implies",
"~" denotes "not",
r is a true statement describing properties that exist if *p* is true, and
s is a true statement describing properties that exist if ~*p* is true.

The truth table for (1) yields (true ⇒ false), which is a false implication. So it is false that the comparison of the two cases, *p* and ~*p,* implies that both exist simultaneously.

The truth of the following two sentences in itself confirms the validity of the comparison strategy:

If a mathematician writes, on a sheet of paper, "If p, then ... " and below that, on the same sheet of paper, he writes, "If not-p, then ... " he has not thereby written a contradiction.

If in the first "...", he shows that the integer *w* has the property *U*, and in the second "..." he shows that *w* has the property not-*U*, he has not thereby asserted that *w* has both the properties *U* and not-*U*.

Other refutations of the claim that comparison implies simultaneous existence, are given in item (3) of the section, "Important Preliminary Remarks" in our paper, "A Solution to the $3x + 1$ Problem", on occampress.com, and in our short paper, "Is It Legitimate to Begin a Sentence With 'If Counterexamples Exist, Then...' ", on occampress.com.

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

For each $k \geq 1$, let $U(k, a, b, c) = a^k + b^k - c^k$, where *a*, *b*, *c*, *k* are positive integers.

Definition of Fixed-Set *F*

We begin with an example.

We cannot seriously imagine a professional mathematician saying, prior to Wiles' proof of FLT, things like, "Well, of course we know that $17^3 + 6^3 - 19^3 = -1730$, not 0, but if a counterexample is proved to exist, then this might change — the value on the right-hand side might no longer be -1730."

Thus, we say that $17^3 + 6^3 - 19^3 = U(3, 17, 6, 19)$ is an element of the *Fixed-Set F*, because the value of $17^3 + 6^3 - 19^3$ 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 (and hence for all exponents) less than 4,000,000. 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. 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 $U(k, a, b, c)$ into two sets:

(1) the set $F = \{U(k, a, b, c) \mid a^k + b^k - c^k$ is the same regardless whether a counterexample

exists or not (for this reason, we call F 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.

In this section, we assume that a counterexample $x^p + y^p - z^p = 0$ exists, and we define our Fixed-Set to include at least the set $\{U(1, x, y, z), U(2, x, y, z), \mathrm{U}(3, x, y, z), ..., U(p - 1, x, y, z)\}$.

First Version of Fixed-Set Approach

By basic algebra, it is easy to show that there exists a $g(x, y, z)$ such that

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

where $g(x, y, z)$ is an algebraic expression involving products of powers of x, y, z. In fact, if we multiply out the product on the left-hand side of (1), we get $x^p + y^p - z^p$ + (a set of terms which we call $(-g(x, y, z))$), yielding Equation (1). It follows that:

(2)
$$x^{p-1} + y^{p-1} - z^{p-1} = (x^p + y^p - z^p - \mathrm{g}(x, y, z))/(x + y + z).$$

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 counterxample. Thus a member of the Fixed-Set is a member of its complement, a contradiction. And thus FLT is proved.

Remark

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, the value of $U(p, x, y, z)$ would have no influence on the value of $U((p - 1), x, y, z)$ or on the value of any other $U(k, x, y, z)$.

Second Version of Fixed-Set Approach

If a counterexample exists, then for each $q > p$ we have a congruent set mod q with $U(p, x, y, z)$ as base element. The elements of that set are all $U(p + j(q - 1), x, y, z)$, where j is a non-negative integer, and each such U except for the base element is a multiple of q. However, if a counterexample does not exist, there is no such p, and therefore the congruent sets are not the same.

Extension of the Fixed-Set

Let q be any modulus $> p$. By definition, $U(1, x, y, z) = x + y - z$. It can be shown by elementary, but tedious, algebra that for each $k \geq (1 + q - 1)$, there exists an algebraic expression $A(x, y, z)$ composed of terms in x, y, z with integer coefficients. such that $(x + y - z)^k - A(x, y, z) = x^k + y^k - z^k$. We are concerned in particular with $k = 1 + j(q - 1)$ for any positive integer $j \geq 0$, that is, with k congruent to 1 mod $(q - 1)$, or, in other words, with k that are exponents of U in the congruent set mod q having $U(1, x, y, z)$ as base element.

We claim that $x^k + y^k - z^k$ is the same regardless if a counterexample exists or not, for the reason that the algebra that produced $A(x, y, z)$ is independent of whether a counterexample exists or not. Thus all elements of the congruent set having $U(1, x, y, z)$ as base element are in the Fixed-Set.

Proof That Elements of ~*F* Are In *F*, a Contradiction

Now let us consider the elements of the congruent set having $U(p, x, y, z)$ as base element. They are of the general form $U(p + v(q - 1)(q_1 - 1)(q_2 - 1)...(q_n - 1), x, y, z)$ with value $wqq_1q_2...q_n$. But that value is a direct consequence of the fact that $U(p, x, y, z) = 0$, hence all elements of its congruent class are multiples of q, for all odd prime moduli q.

So, on the basis of "" on page 28, we assert that at least one element of the congruent set having $U(1, x, y, z)$ as base element, is different as a result of there being a counterexample — meaning, is not the same as it would be if a counterexample did not exist. But this means that elements of ~*F* are in *F*, a contradiction. If our reasoning is correct, we have a proof of FLT.

Third Version of Fixed-Set Approach

By definition of Fixed-Set, each of $U(1, x, y, z)$, $U(2, x, y, z)$, $U(3, x, y, z)$, ..., $U(p - 1, x, y, z)$ is an element of the Fixed-Set.

But now consider the prime modulus $q = 3$. Here, as we showed under "Fact About the Factor $(3 - 1)$" on page 30, all $U(k, x, y, z)$ such that k is odd, are in the congruent set whose base element is $U(1, x, y, z)$. But $U(p, x, y, z)$ is in this congruent set, and so each of $U(1, x, y, z)$, $U(3, x, y, z)$, $U(5, x, y, z)$, ..., $U(p - 2, x, y, z)$ is *not* in the Fixed-Set. If our reasoning is correct, this contradiction gives us a proof of FLT.

Fourth Version of Fixed-Set Approach

1. If $U(p, x, y, z)$ is not a counterexample, then it is a finite product of primes. Thus there is an infinity of primes q (we don't know which ones) such that $U(p, x, y, z)$ is in a congruent set mod q such that $U(p, x, y, z)$ is not a multiple of q. Nor is any $U(p + j(q - 1), x, y, z)$, where j is a positive or negative integer.

2. But what we have said does not apply if $U(p, x, y, z) = 0$. In that case, $U(p, x, y, z)$ is the base element of the congruence *class* all of whose elements are multiples of p. So, trivially, $U(p + j(q - 1), x, y, z)$, where j is a positive or negative integer, is a multiple of q.

3. But this means that some members of the Fixed-Set F are also in the complement of that set, which is a contradiction. These members are the $U(p + j(q - 1), x, y, z)$, where j is a negative value that still leaves a positive exponent. Since these exponents are less than p, they are members of the Fixed-Set. When a counterexample did not exist, they were not a multiple of q, but when a counterexample exists, they are. If our reasoning is correct, this contradiction gives us a proof of FLT.

We remark in passing that *if* the order the values of elements in a congruent set corresponds to the order of elements in a congruence *class*, that is, proceeding from decreasing negative to increasing positive, then we might have a second contradiction, since, if $U(p, x, y, z)$ is a counterexample, and the modulus q is such that $U(p, x, y, z)$ is not a base element of its congruent set, then the value of the elements below $U(p, x, y, z)$ in the congruent set must be negative. But by Lemma 1.5 in Part (1) of this paper, on occampress.com, they must be positive.

However, there is no reason why the order of values of elements in a congruent set should correspond to the order of elements in a congruence class.

Fifth Version of Fixed-Set Approach

1. We first point out a fact about $x^k + y^k - z^k$, where $k \geq 1$, and where x, y, z are constituents of an assumed counterexample.

Let q be an odd prime. Then each $x^k + y^k - z^k$ has a location in the integers mod q. (See "Definition of "Location" of U(k, x, y, z)" on page 8. This location can be conceived of as follows:

the first (lowest) level of $x^k + y^k - z^k$ expressions consists of $x^1 + y^1 - z^1, x^2 + y^2 - z^2, x^3 + y^3 - z^3, ..., x^{q-1} + y^{q-1} - z^{q-1}$;

the second level consists of $x^{1+q-1} + y^{1+q-1} - z^{1+q-1}, x^{2+q-1} + y^{2+q-1} - z^{2+q-1}, x^{3+q-1} + y^{3+q-1} - z^{3+q-1}, ..., x^{q-1+q-1} + y^{q-1+q-1} - z^{q-1+q-1}$;

...

the $(j+1)$th level consists of $x^{1+j(q-1)} + y^{1+j(q-1)} - z^{1+j(q-1)}, x^{2+j(q-1)} + y^{2+j(q-1)} - z^{2+j(q-1)}, x^{3+j(q-1)} + y^{3+j(q-1)} - z^{3+j(q-1)}, ..., x^{(j+1)(q-1)} + y^{(j+1)(q-1)} - z^{(j+1)(q-1)}$;

...

In general we do not know the value of $x^k + y^k - z^k$, but we do know that the values of all $x^{h+j(q-1)} + y^{h+j(q-1)} - z^{h+j(q-1)}$, where $1 \leq h \leq (q - 1)$ and $j \geq 1$, are congruent mod q.

For each q, the location of each expression $x^k + y^k - z^k$ is the same whether or not a counterexample exists. The value, however, will be different, depending on whether or not a counterexample exists. If a counterexample does not exist, then the value of $x^p + y^p - z^p$ is a finite product of primes.

2. Assume a counterexample $x^p + y^p - z^p$ exists. Then for each $q < p$, the expressions $x^k + y^k - z^k$, where $1 \leq k \leq (q - 1)$, are all on the first (lowest) level. But each of these expressions is in the

Fixed-Set — that is, they have the same value whether or not a counterexample exists, because their exponent is less than p. We can only conclude that each expression in each congruence class mod q likewise has the same value whether or not a counterexample exists[1], because the laws of arithmetic are not subject to the truth or falsity of FLT. But $x^p + y^p - z^p$ is an expression in one of these congruence classes, and therefore it must have the same value whether or not it is a counterexample/

3. But then there is no difference between the values of expressions if a counterexample exists, and the values of expressions if a counterexample does not exist, from which we conclude that the set of counterexamples is empty.

If our reasoning is correct, we have another proof of FLT.

Sixth Version of Fixed-Set Approach

Note: at present, we question the validity of this Approach, because what we say about the counterexample case would also apply if there were no counterexample but if the factors of the values of all $U(p, x, y, z)$ were the set of all primes.

1. If FLT is true for the exponent k, then it is true for all multiples of k. For, if it is true for k, then for all positive integers a, b, c, $a^k + b^k \neq c^k$. This includes the positive integers $a = u^n$, $b = v^n$, and $c = w^n$, where u, v, w, n are positive integers. But then we have

$$u^{n^k} + v^{n^k} \neq w^{n^k}$$

or

$$u^{nk} + v^{nk} \neq w^{nk}$$

So all $U(nk, x, y, z)$, where $k < p$, the odd prime exponent in the assumed counterexample, and n is a positive integer, and x, y, z, are constituents of the assumed counterexample, are in the Fixed-Set.

(From here on in this Version, x, y, z, p will always be the constituents of an assume counterexample to FLT.)

2. Our strategy in this Version will be to show that, if C is a congruent set mod q having the counterexample $U(p, x, y, z)$ as base element, then there are $U(k, x, y, z)$ in C for which k is a multiple of a prime less than p. Thus $U(k, x, y, z)$ is both not in, and in, the Fixed-Set. If our reasoning is correct, this contradiction gives us a proof of FLT.

---

1. We know for another reason that there is an infinity of expressions in the various congruent classes mod q that are elements of the Fixed-Set. The reason is that if FLT is true for an exponent, for example, an exponent h, where $1 \leq h \leq (q - 1)$, then it is true for all multiples of h. Hence $x^{hn} + y^{hn} - z^{hn}$ is an element of the Fixed-Set. (See step 1 of "Fifth Version of Fixed-Set Approach" on page 38.)

Statement (D)

Let p be the odd prime exponent in the assumed counterexample. Then there exists a countable infinity of prime moduli q'', where q'' is a prime greater than p, and, for each such modulus, there exists a countable infinity of w, though not consecutive w, where $w \geq 1$, such that the exponent $(p + w(q'' - 1))$ in $U((p + w(q'' - 1)), x, y, z)$ has an odd prime factor less than p.

Proof:

D1. Let $N = 3 \bullet 5 \bullet 7 \bullet \ldots \bullet p'$, where p' is the largest prime less than p. In other words, N is the product of all odd primes less than p.

D2. Consider the set of congruence classes mod N. By Dirichlet's Theorem, there exists an infinity of primes q in the congruence class 1 mod N. For each of these q, $(q - 1)$ is a multiple of N.

Let $\varphi(n)$ be Euler's totient function. (This function returns the number of integers less than n that are relatively prime to n.) In our case, $\varphi(N) > 1$, because there are primes greater than p' and less than N.

Thus there exist other congruence classes besides 1 mod N that are relatively prime to N. Among these are those whose minimum residues are primes q', where $p < q' < N$. By Dirichlet's Theorem, we know there is an infinity of primes q'' in each such congruence class. For each of these primes q'', $(q'' - 1)$ is not a multiple of N (only the integers $(q - 1)$, where q is in the class 1 mod N, have that property). That is, there are prime factors of N that are not in these $(q'' - 1)$. (If there were no such factors, then $(q'' - 1)$ would be a multiple of N, a contradiction.) Let these prime factors be denoted $p_1, p_2, \ldots, p_i, \ldots, p_h$.

D3. Now consider $(q'' - 1)$ as a modulus. For each p_i, $(p_i, (q'' - 1)) = 1$, as we have just established. A basic result in elementary congruence theory states that:

If m is a modulus and r is relatively prime to m, that is if $(m, r) = 1$, then the sequence of products $1r, 2r, 3r, 4r, \ldots, mr$ cycles through all m congruence classes. If we continue the sequence with $(m+1)r, (m + 2)r, \ldots, (m + m)r$, we cycle through the congruence classes in the same order, etc. So each congruence class contains an infinity of multiples of r.

In our case, r is one of the p_i.

D4. We know that p, the exponent in $U(p, x, y, z)$, must be an element of one of the congruence classes mod $(q'' - 1)$, say, the class containing one of the infinity of multiples of p_i. The reason is that each positive integer is an element of one of these classes, and so p must be. Hence there exists an infinity of w, though not consecutive w, such that for each w, there is a u such that $p + w(q'' - 1) = up_i$. And p_i, by definition, is a prime less than p. □

(We are indebted to a graduate student for the original version of this proof. However, all errors in the above re-written version are entirely our own.)

3. If a counterexample does not exist, then:
$U(p, x, y, z)$ is a finite product of primes q.
For each of these primes q:
$U(p, x, y, z)$ is in the congruence class C mod q whose minimum residue is zero.

Each element in the set $\{U((p + j(q - 1)), x, y, z)\}$ where $j \geq 1$, is in the class C and therefore is a multiple of q.

For the infinite set of primes q' not equal to one of these primes q, each element in the set $\{U((p + j(q' - 1)), x, y, z)\}$ is *not* a multiple of q'.

On the other hand:
If a counterexample exists, then
$U(p, x, y, z) = 0$.
For each prime q (here q is any prime, not just one of a finite number of primes):
$U(p, x, y, z)$ is in the congruence class C whose minimum residue is zero.
Each element in the set $\{U((p + j(q - 1)), x, y, z)\}$ where $j \geq 1$, is a multiple of q.

So we see that there is only a *finite set* of prime moduli (namely, those prime moduli that are factors of $U(p, x, y, z)$ if a counterexample does not exist), such that, for each modulus, the elements of the congruence class C whose minimum residue is zero, are in the Fixed Set.

But Statement (D) implies there is an *infinite set* of moduli such that, for each modulus, the elements of the congruence class C whose minimum residue is zero, are in the Fixed Set.

If our reasoning is correct, then this contradiction gives us a proof of FLT.

Seventh Version of Fixed-Set Approach

If FLT Is True For the Exponent *k*, It is True For All *nk*

1. If FLT is true for the exponent k, then it is true for all multiples of k. For, if it is true for k, then for all positive integers a, b, c, $a^k + b^k \neq c^k$. This includes the positive integers $a = u^n$, $b = v^n$, and $c = w^n$, where u, v, w, n are positive integers. But then we have

$$u^{n^k} + v^{n^k} \neq w^{n^k}$$

or

$$u^{nk} + v^{nk} \neq w^{nk}$$

Review of Definition of the Fixed-Set

2. Prior to Wiles' proof of FLT, FLT had been proved true for all exponents less than 4,000,000. Thus the minimum prime p in a counterexample would have to be greater than 4,000,000.

Assume a counterexample $x^p + y^p - z^p = 0$ exists. We call each $U(k, x, y, z)$ such that $k < p$, an element of the *Fixed-Set*, because the value of $U(k, x, y, z)$ is the same whether or not a counterexample exists. (We cannot seriously imagine a professional mathematician saying, prior to Wiles' proof, 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!"

3. So, from step 1, we can assert that all $U(nk, x, y, z)$, where k is prime and $k < p$ and n is a positive integer and p is the odd prime exponent in the assumed counterexample, $x^p + y^p - z^p = 0$ — all these $U(nk, x, y, z)$, are in the Fixed-Set.

Summary of Our Strategy

2. Our strategy in this Version is to show that, if a counterexample exists, then there are $U(k, x, y, z)$ that are both in, and not in, the Fixed-Set, a contradiction that gives us a proof of FLT.

Review of Location vs. Value of $U(k, x, y, z)$

3. Before we begin our argument, we must emphasize that, for each prime modulus q, there is exactly one set of congruent sets mod q. Specifically, each $U(k, x, y, z)$ is in exactly one location in exactly one congruent set mod q. The *value* of a $U(k, x, y, z)$ may differ, depending on whether a counterexample exists or not, but the *location* of each $U(k, x, y, z)$ is always the same, whether a counterexample exists or not. (For further details, see "Definition of "Location" of U(k, x, y, z)" on page 22.)

If a Counterexample Does Not Exist...

4. Assume a counterexample does not exist.

5. Then each $U(k, x, y, z)$ is a finite product of primes. Choose a particular k, and call these primes $q_1, q_2, \ldots q_i, \ldots, q_n$.

6. Now consider the modulus q_i.

For each j, where $j \geq 0$, each $U((k + j(q_i - 1)), x, y, z)$ is a multiple of q_i. because all the exponents are congruent mod $(q_i - 1)$.

7. But since $j \geq 0$, j can equal $(w(q_1 - 1)(q_2 - 1)\ldots (q_n - 1))$ where w is a positive integer.

And so we can assert that $U((w(q_1 - 1)(q_2 - 1)\ldots (q_n - 1)), x, y, z)$:

is an element of the congruent set mod q_1, all of whose elements are multiples of q_1, and also
is an element of the congruent set mod q_2, all of whose elements are multiples of q_2, and also
...
is an element of the congruent set mod q_n, all of whose elements are multiples of q_n.

8. These q_i are the only moduli q such that $U(k + (w(q_1 - 1)(q_2 - 1)\ldots (q_n - 1))(q_i - 1), x, y, z)$ is an element of a congruent set mod q all of whose elements are multiples of q.

9. Since w is a positive integer, there is an infinity of these $U(k + (w(q_1 - 1)(q_2 - 1)\ldots (q_n - 1))(q_i - 1), x, y, z)$ in each congruent set mod q_i.

If a Counterexample Exists...

10. Assume a counterexample exists.

Then what we have said in steps 4 - 9 applies not just to a finite set of prime moduli, but to *all*

prime moduli.

That is, for *each* prime q, there is an infinity of $U((k + j(q - 1)), x, y, z)$ that are elements in the congruent set mod q' such that all elements in that congruent set are multiples of q'. Here, q' is any prime modulus.

11. Now assume $U(p, x, y, z) = 0$ is a counterexample. and let q be any prime modulus. Let k be any prime less than p.

12. If a counterexample exists, then for each prime q, each $U(p + j(q - 1), x, y, z)$ is a multiple of q, where $j \geq 1$. The consequent is not true for each prime q if a counterexample does not exist.

13. Since we have an infinity of q to choose from, we can find a q such that k (which is a prime less than p), $q - 1$, and p are relatively prime in pairs.

14. Now the infinite sequence of exponents $1k$, $2k$, $3k$, $4k$, … cycles infinitely often through all the congruence classes mod q. Therefore, there exists a w such that for some n, $p + w(q - 1) = nk$.

A Contradiction

15. But then an element of the Fixed-Set, namely, $U(nk, x, y, z)$, is also not a member of the Fixed-Set, since $nk = p + w(q - 1)$ and $U(p + w(q - 1), x, y, z)$ is not in the Fixed-Set. If our reasoning is correct, then we have a proof of FLT.

Application of The Fixed-Set Approach to Another Very Difficult Problem

The Fixed-Set Approach also seems applicable to a proof of the $3x + 1$ Conjecture. See "Most Recent Proof of Conjecture", "First Proof", "Second Proof" and "Third Proof" in "A Solution to the $3x + 1$ Problem" on www.occampress.com. It also seems applicable — though we make no claims — to a possible proof of Goldbach's Conjecture. Our reasoning is given below.

Note: readers who are still skeptical about the Fixed-Set Approach and, in particular, about the comparison of mutually-exclusive cases, are strongly urged to *first* read the section, "(3) Common Misconceptions About the Nature of the Comparison of Mutually-Exclusive Cases" in the above paper.

Goldbach's Conjecture

Goldbach's Conjecture states that each even positive integer greater than 4 is the sum of two odd primes.

A Fixed Set Approach to a Proof

Note: The section, "A Word Regarding a Certain Type of Objection to This Approach" on page 34 applies here also.

1. Consider an infinite matrix M (see Table 1). The columns are labeled 3, 5, 7, 11, …, and similarly for the rows. Thus, the column labels are all the odd primes in increasing order, and similarly for the row labels.

Definition: We define an *n-square* to be the square established by the first n columns and the first n rows in M. The cell (r, c) contains the sum $p_r + p_c$, where p_r is the rth odd prime and p_c is the cth odd prime. The matrix in Table 1 shows the 5-square. Observe that all even numbers ≤ 26 except 4 (which is not the sum of two odd primes) are contained in the 5-square.

Table 2: Example of an *n*-square: here *n* = 5

	3	**5**	**7**	**11**	**13**	**...**
3	6	8	10	14	16	...
5	8	10	12	16	18	...
7	10	12	14	18	20	...
11	14	16	18	22	24	...
13	16	18	20	24	26	...
...	...	...	...	...	...	...

2. Let M_{nco} denote a matrix in which the rows and columns are the odd primes, and such that the contents of the cell at $(r, c) = p_r + p_c$, and such that M_{nco} contains no counterexample to the Conjecture, that is, such that every even, positive integer is in M_{nco}.

Let M_{co} denote a matrix in which the rows and columns are the odd primes, and such that the contents of the cell at $(r, c) = p_r + p_c$, and such that M_{co} contains a counterexample to the Conjecture, that is, such that a positive even integer is missing from M_{co}.

The two matrices are *different* if a counterexample exists! Matrix M_{nco} contains all even positive integers, matrix M_{co} does not.

Let S denote the largest set of *successive* even numbers that are known to be the sum of two primes. We call S the *Fixed-Set*. Let n be the smallest n such that the n-square contains S.

Each element s in S is in the n-square, and is the sum of two primes, p_r and p_c. *This sum is the same whether or not a counterexample to the Conjecture exists.* Thus, for example, 18 = 7 + 11, a fact that is true today, and will be true if the Conjecture is proved true tomorrow, and will be true if the Conjecture is proved false tomorrow.

3. It is easy to show that (informally) for all $k \geq 1$, the numbers in row $k + 1$ are the numbers in row $k + (p_{k+1} - p_k)$, and similarly for the numbers in column $k + 1$. More precisely (see above Table), the even number in cell $(k + 1, c)$ = the even number in cell $(k, c) + (p_{k+1} - p_k)$. Thus the even number in cell (5, 3) = 20, and 20 = 18 + (13 – 11).

By step 3, for all $m > n$, row m is the same in both matrices M_{nc} and M_c and similarly for column m. Therefore each m-square in M_c is the same as each m-square in M_{nc}. We conclude that this implies no counterexample exists.

Conjectures Motivated by the *n*-Square Concept

Examination of all *n*-squares up to $n = 10$ (the rows and columns for which are 3, 5, 7, ...,, 29, 31) suggests the following conjectures:

Conjecture 1: For each *n*-square such that the primes that are the headings of the last two rows and columns are twin primes (that is, primes that differ by 2), all even numbers $\leq n^2$ are in the *n*-square.

If this Conjecture were true, and if it were known that there is an infinity of twin primes, then we would have a proof of Goldbach's Conjecture.

Conjecture 2. For each *n*-square such that the primes that are the headings of the last two rows and columns differ by *k*, where $k > 2$, there exists a function $f(n, k) = m$ such that the *m*-square contains all even numbers $\leq n^2$.

If this Conjecture were true, we would obviously have a proof of Goldbach's Conjecture.

.

Important Questions Regarding Congruent Sets

Is a Congruence Class "Missing" From the Set of Congruent Sets?

For each modulus *q*, there are $q - 1$ congruent *sets*. But there are *q* congruence *classes* mod *q*, by a basic fact of congruence theory. Is a class "missing" from the set of congruent sets? If not, why not?

Answer: No, a class is not missing. It is easily shown that a congruent *set* mod *q* can contain multiples of *q*.

Can Two or More Congruent Sets Occupy a Single Congruence Class?

According to a graduate student, the answer is yes. His argument is that although each congruent set consists solely of elements of one congruence class, there is no reason why two or more congruent sets cannot consist of elements of one and the same congruence class. However, members of one congruent *set* cannot occupy more than one congruence *class*.

What Can We Say About the Value of $U(k, x, y, z)$ When k Does Not Equal $p + j(q - 1)$?

The $U(k, x, y, z)$ we are referring to here are those in congruent sets mod *q* having base element $U(i, x, y, z)$, where $1 \leq i \leq (q - 1)$ but $i \neq p$. We know only that, for a given *i*, the elements of the congruent set are $U(i + j(q - 1), x, y, z)$, where $j \geq 1$, and the values of the elements of the congruent set are congruent mod *q* and are not multiples of *q*.

What Is the Difference in Value Between Successive Elements of the $U(p, x, y, z)$ Congruent Set? Of Any Congruent Set?

In the mod *q* congruent set having $U(p, x, y, z)$ as base element, what is the difference between the value of $U(p + j(q - 1), x, y, z)$ and the value of $U(p + (j + 1)(q - 1), x, y, z)$, other than that the absolute value of the latter must be greater than the absolute value of the former[1] and the values

1. Lemma 1.5 in Part (1) of this paper, on occampress.com

must be multiples of q? Similar questions apply to each of the other $(q - 2)$ congruent sets mod q.

What About Exponents k Containing Powers of $(q - 1)$ in the $U(p, x, y, z)$ Congruent Set Mod q?

How does such an exponent affect the value of the corresponding U?

Is There a Way of Resolving the Ambiguity in Exponent Factors Described in the Section, "Second Version of Approach: Show That a U(p, x, y, z) Congruent Set Element is "Missing"" on page 31?

As we point out in the referenced section, the ambiguity exists in all congruent sets mod q, not just in the congruent set having $U(p, x, y, z)$ as base element. Thus it appears that the ambiguity cannot be the basis of a proof of FLT.

Our best attempt at resolving the ambiguity at present is to simply argue as follows:

For each modulus q, the set of all U in the congruent set having $U(p, x, y, z)$ as base element is the set of all U having exponent $k = p + j(q - 1)$, where j is a non-negative integer. This rule holds regardless of the factors of j.

Probably far more important is the fact that the ambiguity exists even if a counterexample does *not* exist! At present, we believe there is no ambiguity: the location of each $U(k, x, y, z)$ in a congruent set mod q is established in the way we described in the proof of statement (2) in "Basic Facts About U(k, x, y, z) And Congruent Sets" on page 21. That is, the location is simply (i, *level*), where i is the remainder of k/q, and *level* is the quotient of k/q. Thus i is the exponent of the base element $U(i, x, y, z)$ of a congruent set mod q, and *level* is the level in the set.

Therefore, at present, we believe that an approach based on exponents is not worth pursuing. Instead, we should concentrate on approaches based on the values of the $U(k, x, y, z)$.

What Is the Difference Between Mod q Congruent Sets if a Counterexample Exists/Does Not Exist?

For each prime modulus q, what is the difference between the set of all mod q congruent sets if a counterexample exists, and the set of all mod q congruent sets if a counterexample does not exist. (Observe that the term *prime modulus* has meaning whether or not a counterexample exists.) Answers to this question is given in "Approach: Compare U(k, x, y, z)'s if a Counterexample Exists/Does Not Exist" on page 33 and "Second Version of Fixed-Set Approach" on page 37.

What Is the Nature of w in the Value of $U(p + j(q - 1), x, y, z)$?

In general, the value of U equals w times some product of primes. But w can also be a product of primes. So the question arises, can we tell, just by looking at the value of a U, what its exponent k is? What mechanism enables the various U to keep track of the primes in their values that pertain to their exponents?

Why Should It Be Possible for $U(p - 1, x, y, z)$ Not to Equal 0 But for $U(p, x, y, z) = 0$?

Fix a, b, c and consider all $a^k + b^k - c^k$, where $k \geq 3$. Obviously, the set of primes in a^k is the same for all k, and similarly for b^k and c^k. Why should we believe that the mere incrementing of the exponent k can produce an equality, when the primes in all three terms are exactly the same as

they were when there was no equality?

Question Regarding $2c = q - 1$

Does there exist an infinity of pairs (c, q), where c is an odd composite number and q is prime, such that $2c = q - 1$?

How Do We Know That $U(p + j(q - 1), x, y, z)$ Is Always in the "Right Place" in the "Right" Congruent Set?

For an attempt to show that there exists a $U(p + j(q - 1), x, y, z)$ that is *not* in the right place, see "Second Version of Approach: Show That a U(p, x, y, z) Congruent Set Element is "Missing"" on page 31. However, we have become skeptical about any approach based on the possibility of $U(k, x, y, z)$ being in the "wrong place". See "Checklist to Avoid Futile Approaches" on page 28.

How Do We Know That the Value of Any $U(p + j(q - 1), x, y, z)$ Is Correct?

For an attempt to show that the value of at least one $U(p + j(q - 1)$ is *not* correct, see "First Version of Approach: Show a U(k, x, y, z) Has Two Different Values" on page 29.

Approaches Via D-Sets

Note: This section was written well before the previous sections. It was written *after* the section "Approaches Via C-Sets" on page 49.

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:

$\mathbf{D}_{u, v, w, j, q} = \{a^r + b^r - c^r = U(r, a, b, c) \mid a, b, c \equiv u, v, w \bmod q$, respectively, where u, v, w are the minimum residues of congruence classes mod q, $r \equiv j \bmod (q - 1)$; where j is an element of $\{0, 1, 2, 3, ..., q - 2\}$, so that, by Fermat's Little Theorem, $a^r \equiv u^j$, $b^r \equiv v^j$, $c^r \equiv w^j \bmod q\}$.

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 $r \equiv j \bmod (q - 1)$ for each j.

Definition of Complete Set of D-sets

We define a complete set of **D**-sets to be $\{\mathbf{D}_{u, v, w, j, q} \mid j$ is an element of $\{1, 2, 3, ..., q - 1\}\}$.

Basic Facts About D-sets

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 $<u, v, w>$ 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 $a^r \equiv u^j$, $b^r \equiv v^j$, $c^r \equiv w^j$ mod 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 $<a, b, c>$ 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 $<x, y, z>$, where x, y, z are the constituents *o*f a counterexample if a counterexample exists.

(E) For each ordered triple $<a, b, c>$, and for each prime modulus q:

$a \equiv u \bmod q$ for some minimum residue u,
$b \equiv v \bmod q$ for some minimum residue v,
$c \equiv w \bmod q$ for some minimum residue w,

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

and therefore

$a^2 \equiv u^2 \bmod q$,
$b^2 \equiv v^2 \bmod q$,
$c^2 \equiv w^2 \bmod q$,

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

...

$a^{q-1} \equiv u^{q-1} \bmod q$,
$b^{q-1} \equiv v^{q-1} \bmod q$,
$c^{q-1} \equiv w^{q-1} \bmod q$,

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

(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 $\{1, 2, 3, ..., j - 1\}$ 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 mod 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 mod 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 54.

D-set Approach Type I: Approach Via the Fixed-Set

This Approach is set forth in "Approaches Using Only Powers of x, y, z (Congruent Sets)" on page 19.

Approaches Via C-Sets

Note: This section was written well before the previous section.

Definition of C-set

C-sets are an earlier version of **D**-sets, and are similar to *towers* in previous versions of this paper.

We want to capture, for each modulus m such that $(x, m) = (y, m) = (z, m) = 1$, certain ordered pairs $<a^r + b^r, c^r>$, where $(a, m) = (b, m) = (c, m) = 1$. We do this with **C**-sets. These exploit both Fermat's Little Theorem and (1.91)(c), which are described above under "Fermat's Little Theorem" on page 51 and "(1.91) (c)" on page 51. For a modulus $m \geq 2$, we define a **C**-set $\mathbf{C}_{u, v, w, j, m}$ mod m as follows:

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

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

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

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

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

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

Summary of Approaches Via C-Sets

C-set Approaches Type I through V

(Type I) Show that if $x^p + y^p = z^p$, then a contradiction arises involving $a^p + b^p$, c^p, where $a \leq x$, $b \leq y$, $c \leq z$, and $a \equiv x$, $b \equiv y$, $c \equiv z$ mod m. This Approach is the same as Approach Type II, except that instead of our exponent $r \equiv p$ mod $\varphi(m)$, we have simply the exponent p.

(Type II) Show that if $x^p + y^p = z^p$ then a contradiction arises involving $x^r + y^r$, z^r , where $2 < r < p$. If m is an appropriate modulus, then it must be the case that $r \equiv p$ mod $\varphi(m)$. If $x^r + y^r$, z^r are each less than m, then we have a proof of FLT, because if $x^r + y^r = z^r$, then we have a counterexample with an exponent r less than p, contrary to the fact that our counterexample is minimum. If $x^r + y^r \neq z^r$, then $x^p + y^p$ not $\equiv z^p$ mod m, which is not possible if $x^p + y^p = z^p$. So our only task is to show that an appopriate modulus m exists such that $x^r + y^r$ and z^r are each less than m.

We might be able to combine the first two Approaches, and thus allow a smaller appropriate modulus, but we must first show that, in that case, it would be true that $a + b \neq$ c and $a^2 + b^2 \neq c^2$. These two conditions are true for a, b, $c = x$, y, z respectively.

(Type III) This is now an approach using **D**-sets. See "Approaches Via D-Sets" on page 47.

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

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

Supporting Material for C-set Approaches I - V

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

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

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

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

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

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

Example:

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

(3)

If $a + b \equiv$ c mod m, then

(a) if $a + b$, c are each less than m, then $a + b = c$;

(b) if one of $a + b$, $c > m$, then $a + b \neq c$.

Informally: "Congruence implies equality for sufficiently large modulus."

(4)

If $a + b$ not $\equiv$ c mod m, then $a + b \neq c$.

Informally: "Non-congruence implies inequality."

Fermat's Little Theorem

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

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

Another Fundamental Result We Will Use

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

(1.91) (c)

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

$a \equiv a' \bmod m$, *and* $b \equiv b' \bmod m$, *and* $c \equiv c' \bmod m$, *then*

if $a^r + b^r \equiv c^r \bmod m$, $r \geq 1$,

then $a'^r + b'^r \equiv c'^r \bmod m$ *and*

$a^r \equiv a'^r \bmod m$ *and* $b^r \equiv b'^r \bmod m$ *and* $c^r \equiv c'^r \bmod m$.

(See "(1.91)(c)" in Part (2) of this paper, on the web site occampress.com.)

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

---

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

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 51. Suppose that q is a prime such that $(x, q) = (y, q) = (z, q) = 1$, and suppose that $p \equiv j \bmod (q-1)$, where $1 \leq j \leq q-1$ and where $p > j$. In other words, suppose $p = j + k(q-1)$, where $k > 0$. (The question whether such a q exists is discussed in the section "Moduli — Notation" on page 52.) Then by Fermat's Little Theorem:

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

Now if we can show that the last case in the sequence is such that $x^j + y^j$ and z^j are each less than q, then we have a 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 $q^1, q^2, q^3, ..., q^k, ...,$ 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 51. 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 $x^p + y^p \equiv z^p \bmod q$ (non-congruence would imply inequality). Then for all a', b', c' such that $a' \equiv x$, $b' \equiv y$, and $c' \equiv z \bmod q$, and $a' \leq x$, and $b' \leq y$, and $c' \leq z$, where at least one "≤" is "<", we have, by (1.91)(c) that $a'^p + b'^p \equiv c'^p \bmod q$.

Now if we can show that there exists a', b', c' such that $a'^p + b'^p$ and c'^p are each less than q, and such that at least one of $a', b', c' \neq x, y, z$ respectively, then 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 counterxample (via at least one of a', b', c') than our assumed minimum counterexample $x^p + y^p = z^p$. Either contradiction gives us a proof of FLT. Both contradictions could be avoided if a similar condition prevailed as was described in the previous paragraph. This 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 — Notation

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

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

The Vertical Approaches via the "Lines-and-Circles" Model of Congruence will make frequent use of a sequence of moduli, $q^1, q^2, q^3, ..., q^k, ...$, where q is a prime such that $(x, q) = (y, q)$

= $(z, q) = 1$. As the reader will see, it is important that q be such that at least one of $x + y$, z be greater than q. For a 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 $x = 2 \bullet 3 \bullet 5 = 30$, let $y = 7 \bullet 11 = 77$, 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 4,000,000, 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 countereexample. So there may be grounds for cautious optimism that we can prove that there exists a prime modulus q such that $(x, q) = (y, q) = (z, q) = 1$ and $q < x$.

A proof that a q exists that is less than y, or less than x, is given in "Lemma 30.0: Statement and Proof" in 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 C-set Approaches I - V" on page 50 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 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 $\equiv z^k \mod m$. For if $x^k + y^k \neq z^k$ (as is indeed the case if $k \neq p$) then $x^k + y^k + U_k = z^k$, where U_k is not 0. Then for all moduli m such that U_k is not a multiple of m, it is the case that $x^k + y^k$ not $\equiv z^k \mod m$.

Trade-offs in the Size of Moduli

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

On the other hand, 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.

Conditions for Existence of a Counterexample

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

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

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

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

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

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

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

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

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

"Consequences" of a Counterexample

Readers who first contemplate the infinite sequence of cases,

$x^1 + y^1 \neq z^1$,

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

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

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

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

In fact, we can say more:

Lemma 60.0:

Assume a counterexample $x^p + y^p = z^p$ exists.

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

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

$r \equiv k \bmod q - 1$,
then $x^r \equiv x^k, y^r \equiv y^k, z^r \equiv z^k \bmod q$.
The other is via "(1.91) (c)" on page 51, which implies that if
$a \equiv x \bmod q$, and $b \equiv y \bmod q$, and $c \equiv z \bmod q$, *and if*
$x^r + y^r \equiv z^r \bmod q$, *then*
$a^r + b^r \equiv c^r \bmod q$.

For all $k \geq 1$, and for all positive integers k, a, b, c, such that $<a^r, b^r, c^r>$ is *congruent to the triple $<x^k, y^k, z^k>$, 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.

Proof:

See "Lemma 60.0: Statement and Proof" in Part (2) of this paper, on the web site www.occam-press.com.

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 $<nx^p + ny^p , nz^p>$ is the base element of a **C**-set mod q^{k+j} . By definition of **C**-set this means that the **C**-set contains an infinity of congruent elements $<a^r + b^r, c^r>$. *None of these elements would be congruent if the counterexample did not exist.* So the existence of the counterexample has more "consequences".

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

Finally, if a counterexample exists, then for each j, k, l such that $j + k = l$ and such that each of $x^p – jm$, $y^p – km$, and $z^p – lm$ is positive, we have $(x^p – jm) + (y^p – km) = (z^p – lm)$. Each of these *equalities* occurs "below" the counterexample in the sense that each term in parentheses is less than the corresponding term in the counterexample. *These equalities would not exist if the counterexample did not exist.* For further details, see "First Implementation" on page 57, 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 "" on page 70, and in part (E) of "C-set Approach Type IV: Considering All Multiples of All Powers of a, b, c" on page 63.

C-set Approach Type I

Preliminary Discussion

Elementary Fact About Equality, Inequality and Congruence

Assume $a + b = c$. Then for each modulus m, and for each triple j, k, l such that $j + k = l$, then $d + e = f$, where $d = a – jm$; $e = b – km$, 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. Con-

sider 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).

.Similarly, if $a + b \neq c$, then if we subtract the same number from the left-hand and right-hand sides of the inequality, we arrive at another inequality. So if in fact $a + b \neq c$ (where a, b, c are very large numbers), but we assume that $a + b = c$, then with suitable subtractions, we can end up with an inequality of sufficiently small numbers that we can recognize the inequality, and thus our error will be revealed to us. Obviously, this suggests an approach to a proof of FLT, with $a = x^p$, $b = y^p$, and $c = z^p$.

Implementations of Approach Briefly Described

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

First Implementation: show that a contradiction arises between the amount of "room" required for all $<a^k, b^k, c^k>$ below $<x^p, y^p, z^p>$ that are congruences but *are not* equalities, and $<a^k, b^k, c^k>$ 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 $<a^p, b^p, c^p>$ 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:

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

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

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

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

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

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

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

Second Implementation

If we can show that the assumption of a counterexample imples 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, ..., q_i, ..., 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 $\{<a^p, b^p, c^p> \mid a^p + b^p$ and c^p are each less than $q\}$.

V_q denote the set $\{<a^p, b^p, c^p> \mid a^p \equiv x^p, b^p \equiv y^p, c^p \equiv z^p \ mod\ q\}$.

Part (d) of "Lemma 60.0:" on page 55 imples 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 $<a^p, b^p, c^p>$ in T_q as the sequence of q progresses. Thus, initially we have $<1^p, 1^p, 1^p>$ 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 57.

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

We will attempt to exploit the set of equalities that is established by any equality, as we described above. The equality in our case is the counterterexample. In particular, we will attempt

to arrive at a contradiction between the existence of these *equalities*, and certain congruences that are also established by the counterexample — congruences each of which must be an *inequality.*

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

The Set of Equalities

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

First Set of Congruences

The first set of congruences, each of which represents an *inequality*, is the set $\{x^n + y^n \equiv z^n \bmod m \mid n = p - j \bullet \varphi(m)\ ,\ j \geq 1$, and n is positive$\}$. That these are congruences follows from "Fermat's Little Theorem" on page 51. 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 $\{a^p + b^p \equiv c^p \bmod m \mid a, b, c$ are less than x, y, z respectively and $a \equiv x,\ b \equiv y,$ and $c \equiv z \bmod m\}$. That these are congruences follows from "(1.91) (c)" on page 51. 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 $<u, v, w>$ such that $u < x^p$, $v < y^p$, and $w < z^p$ and $u \equiv x^p$, $v \equiv y^p$, and $u \equiv z^p \bmod m$;
- the number of elements in the subset S_e of S consisting of ordered triples representing equalities, including the equalities resulting from the counterexample as described above;
- the number of elements in the subset S_i of S consisting of ordered triples representing inequalities;
- the number of elements in the subset of $S_{i,c}$ of S_i consisting of ordered triples representing inequalities that are congruences mod m;
- the number of elements in the subset $S_{i,n}$ of S_i consisting of ordered triples representing inequalities that are not congruences mod m.

Two Major Obstacles in the C-set 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. Following is a brief description of each obstacle.

First Obstacle — Does the Right Appropriate Modulus Exist?

We must assume that Lemma 30.0 (see "Lemma 30.0: Statement and Proof" in Part (2) of this paper, on the web site occampress.com) describes a worst-case that our Approaches must deal with, unless results existing prior to 1990 show that the factors of x, y, z in a counterexample need not be all primes $\le z$. We are not aware of any such results. So we must assume that q is a prime such that x, y are each less than q, and $z > q$. [*Note*! This is not necessarily true! See "Moduli — Notation" on page 52. 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 $\varphi(q)$, there exists one **C**-set whose base element is $<u^p + v^p, w^p>$. The reason is that $p < x < q$ implies $p < \varphi(q) = q - 1$. In other words, for each u, v, w such that $u, v, w, < q$ and $(u, q) = (v, q) = (w, q) = 1$, there exists a base element of a **C**-set in which the exponent of u, v, w is p.

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

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

Second Obstacle — Does the Right Appropriate Modulus Exist? (2)

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

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

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

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

By definition of **C**-set there is an infinity of a, b, c such that $a^r + b^r \equiv c^r \bmod q^2$, where $a \equiv x$, $b \equiv y$, $c \equiv z \bmod q^2$, and $r \equiv p \bmod \varphi(q^2)$. (These congruences would not exist if our assumed counterexample did not exist. They are examples of the "consequences" of the existence of a counterexample described under ""Consequences" of a Counterexample" on page 54.)

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 $h \ne 0$.

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 $\equiv c^r \bmod q^k$, hence $a^r + b^r \neq c^r$) and the second type is that in which h *is* a multiple of q^k (in other words, in which $a^r + b^r \equiv c^r \bmod q^k$ even though $a^r + b^r \neq c^r$) .

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

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

Let q be the modulus defined above under "Two Major Obstacles in the C-set Type I - Type III Approaches Using the Lines-and-Circles Models of Congruence" on page 59 and let k be ≥ 1. Then $<x^p + y^p, z^p>$ is an element (not necessarily the base element) of a congruent **C**-set mod q^k. Now consider the sequence of elements,

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

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

Unfortunately, the first and second terms in the elements of sequence (1) cannot possibly cover the set of all *pairs* of residue classes mod q^k of which there are $\varphi(q^k)$. So we must utilize the known non-congruent **C**-sets . These *include* the ones having base element $< u^j + v^j, w^j >$, where $1 \leq j \leq \varphi(q^k)$, and where $u^j + v^j$ is not $\equiv w^j \bmod q^k$. Such a non-congruence is guaranteed to occur if $u^j + v^j$ and w^j are each less than q^k and $u^j + v^j \neq w^j$.

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

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

Remark on Second Attempt

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

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

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

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

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

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

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

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

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

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)

C-set 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 54. In brief, and informally, we ask: if the existence of a counterexample, $x^p + y^p = z^p$, implies the existence of an infinity of equalities, $nx^p + ny^p = nz^p$, where n is a positive integer, is it possible that there is not enough "room" for all these equalities which, if no counterexample existed, would be inequalities?

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

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

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

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

$1u \equiv a_1 \bmod m$;
$2u \equiv a_2 \bmod m$;
$3u \equiv a_3 \bmod m$;
...
$mu \equiv a_m \bmod m$;
$(m + 1)u \equiv a_{m+1} \bmod m$;
$(m + 2)u \equiv a_{m+2} \bmod m$;
$(m + 3)u \equiv a_{m+1} \bmod m$;
...
where the a_i are minimum residues mod m.

Then by a basic fact of congruence theory, $a_1, a_2, a_3, ..., a_m$ is a sequence of all m minimum residues mod m. Furthermore $a_{m+1} = a_1, a_{m+2} = a_2, a_{m+3} = a_3$, etc.

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

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

(1)
$1x + 1y > 1z$;
$2x + 2y > 2z$;
$3x + 3y > 3z$;
...
$n\text{x} + n\text{y} > nz$;
...
By Lemma 0.0 in Part (1), we know that $x + y = z + Kdef$, and so we can write, from (1),

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

(E) Consider a 5-dimensional matrix M such that cell (n, u, v, w, k) is occupied by the value of $nu^k + nv^k - nw^k$, where n, u, v, w, k are positive integers. The matrix makes it possible to speak of the values of neighboring cells, given the value and location of a cell — if we know n, u, v, w, k, then we can compute the value of $nu^k + nv^k - nw^k$, and then *from that value* we can compute the value of, for example, $n(u-1)^k + nv^k - nw^k$, which is the value of one of the cells next to that containing $nu^k + nv^k - nw^k$. In fact, there are 10 cells next to each cell except where one of the arguments = 1, because each of the arguments (or "coordinates") can be increased by 1 or decreased by 1. (Obviously, we can generalize this matrix concept to contain the values of any number-theoretic function having m integer arguments, where $m \geq 1$.)

The fact that the value of the contents of cells adjacent to a given cell can be computed *from the value* of that cell *is important*! *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 Wiles' proof of FLT in the mid-90s, it was known that if a counterexample existed, p would be greater than 4,000,000 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 4,000,000, 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 **C**-sets whose base element is $<x^p + y^p, z^p>$. See ""Consequences" of a Counterexample" on page 54.

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 $u > 4{,}000{,}000$ 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.

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

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

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

Now consider the following table:

Table 3: Relating Certain Congruent Elements of C-sets, and Moduli

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

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

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

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

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

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

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

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

We also remind the reader of the facts concerning an infinite succession of prime moduli, q, q^2, q^3, ..., as discussed under ""Consequences" of a Counterexample" on page 54.

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

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

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

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

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

We can begin our inquiry with $m = 3$. We see immediately that $\varphi(3) = 2$. As of the early nineties, p was known to be greater than 4,000,000, so our first condition is easily met. The problem is that $m = 3$ requires that neither x, y, or z have a factor of 3. (For the time being we ignore possible use of the Trivial Extension to Fermat's Little Theorem.). We can compute the largest modulus m_{max} such that $\varphi(m_{max})$ is less than 4,000,000. Then FLT is true for all x, y, z such that $(x, m) = (y, m) = (z, m) = 1$, where $m \le m_{max}$, and all the **C**-sets in the above set are non-congruent.

Appendix A — Third Promising Approach to a Simple Proof of FLT

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

We define $U(k, a, b, c)$, where k, a, b, c are positive integers, to be $a^k + b^k - c^k$.

Partitioning of *U*(*k*, *a*, *b*, *c*) in Certain Prime Moduli

For fixed a, b, c, let q be an odd prime such that $(a, q) = (b, q) = (c, q) = 1$. (It is possible that q is a very large prime, since all the prime factors of x, y and z might be all the primes up to a very large one.)

Then the following sets of congruent $U(k, a, b, c)$ exist. We call each such set a *congruent set mod q*, or, if q is understood, then simply a *congruent set*.

$\{U(k, a, b, c) \mid k \equiv 1 \bmod q - 1\}$,
$\{U(k, a, b, c) \mid k \equiv 2 \bmod q - 1\}$,
...
$\{U(k, a, b, c) \mid k \equiv q - 1 \bmod q - 1\}$,

The existence of congruent sets follows from Fermat's Little Theorem, which states that if q is a prime, and $(a, q) = 1$, then $a^{q-1} \equiv 1 \bmod q$.

The congruent sets are the same whether or not a counterexample to FLT exists.

Definition of "Fixed-Set", *F*

We begin with an example.

We cannot seriously imagine a professional mathematician saying, prior to Wiles' proof of FLT, things like, "Well, of course we know that $17^3 + 6^3 - 19^3 = -1730$, not 0, but if a counterexample is proved to exist, then this might change — the value on the right-hand side might no longer be -1730."

Thus, we say that $17^3 + 6^3 - 19^3 = U(3, 17, 6, 19)$ is an element of the *Fixed-Set F*, because the value of $17^3 + 6^3 - 19^3$ 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 (and hence for all exponents) less than 4,000,000. The Fixed-Set *F includes* all $U(k, a, b, c)$ such that $k < p$, where p is the assumed (prime) exponent in the minimum counterexample. In particular, it includes all $U(k, x, y, z)$, where $k < p$ 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 $U(k, a, b, c)$ relative to each modulus q, into two sets:

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

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

Important Fact About the Fixed-Set

Prior to Wiles proof of FLT, it was known that FLT was valid for all exponents up to 4,000,000.

It is easy to prove that, if FLT is valid for the exponent k, then it is valid for all exponents nk, where $n \geq 1$. For, if it is true for k, then for all positive integers a, b, c, $a^k + b^k \neq c^k$. This includes the positive integers $a = u^n$, $b = v^n$, and $c = w^n$, where u, v, w, n are positive integers. But then we have

$$u^{nk} + v^{nk} \neq w^{nk}$$

We know that FLT is true for all a, b, c, k, such that $3 \leq k < p$, where p is the prime exponent in our assumed counterexample.

Possible Proof of FLT

1. *Fact*: If q is a prime, and $k < q$, then the sequence $1k$, $2k$, $3k$, $4k$, … , nk, …, cycles through all congruence classes mod q infinitely often.

Proof:
Since q is prime, and $k < q$, a basic result in elementary number theory states that

(1)
If $nk \equiv n'k \bmod q$ then $n \equiv n' \bmod q$.

(This is trivially true if n, n' are multiples of q.)

Hence no two of $1k$, $2k$, $3k$, $4k$, … , qk can be in the same congruence class.

But the same is true for no two of $(q+1)k$, $(q+2)k$, $(q+3)k$, $(q+4)k$,… , $(q+q)$k.
Etc.
□

Thus, for example, if q is 7 and k is 5, the minimum residues mod 7 for 1*5, 2*5, 3*5, 4*5, … are

5, 3, 1, 6, 4, 2, 0, 5, 3, 1, 6, 4, 2, 0, 5, 3, …

as the reader may verify.

2. Assume a counterexample exists.
Let k be a positive integer, where $3 \leq k < p$.
Let q be a prime modulus containing congruent sets, and such that $k < q$.

3. Then the infinite sequence $1k$, $2k$, $3k$, $4k$, ... , nk, ... cycles through all the congruent sets infinitely often.
But then, because we have assumed a counterexample exists, an nk must equal $p + j(q - 1)$ for some j (in fact for an infinite number of j).
But all nk are exponents for which FLT is true (see "Important Fact About the Fixed-Set" on page 68), that is, they are elements of the Fixed-Set. Yet by what we have just said, some of them

are also exponents for which FLT is false, that is, they are not elements of the Fixed-Set. If our reasoning is correct, this contradiction gives us a proof of FLT.