

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

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

Part (2) Proofs of Lemmas Not Proved in Part (1)

by

Peter Schorer

(Hewlett-Packard Laboratories, Palo Alto, CA (ret.))

2538 Milvia St.

Berkeley, CA 94704-2611

Email: peteschorer@cs.com

Phone: (510) 548-3827

Mar. 24, 2010

Appendix A — Lemma 3.0

Lemma 3.0.

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

Proof¹:

First part:

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

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

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

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

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

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

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

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

Second part:

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

1. This proof is an edited version of a proof by Michael O’Neill. Any errors are solely our fault.

Appendix D — Proof of Lemma 6.0

Lemma 6.0

Let p be the smallest prime exponent in a counterexample to FLT, $x^p + y^p = z^p$. Then there exists a prime q such that $(x, q) = (y, q) = (z, q) = 1$ and such that at least one of $x, y, z > q$.

Proof of Lemma 6.0

1. It was known, as of 1990, that the exponent p in a counterexample must be greater than about 125,000. By “Lemma 1.0.” on page 11 of Part (1) of this paper, on the web site occam-press.com, we know that $p < x < y < z$.

2. “Lucas proved...in 1891: y, z have at least two prime factors.”¹

Let P denote all the primes $\leq z$. Let the primes in P be listed in order of increasing magnitude, and let them be designated $p_1 = 2, p_2 = 3, p_3 = 5, \dots, p_t =$ the largest prime in P . If all the primes in x, y, z do not exhaust all the primes in P , then we have our q : it is simply one of the primes in P that is not a factor of x, y , or z .

3. Therefore we must assume that x, y , and z contain all primes in P . If p_t is a factor in a product H of primes $p_j, 2 \leq p_j \leq p_t$, then there exists a prime p' such that $p_t < p' < 2p_t$, by “Bertrand’s Postulate” on page 14 of Part (1) of this paper, on the web site occampress.com.. Clearly, $p' < H$, since all primes are ≥ 2 .

Thus we have our q (namely p') if p_t is a factor in a product H . Therefore, we must assume that $p_t = x$. We now ask if p_{t-1} is a factor of y . By Bertrand’s Postulate, we know that $p_{t-1} < p_t < 2p_{t-1}$, and that therefore there is a prime p'' , $2p_{t-1} < p'' < 4p_{t-1}$. So if

$$y = p_{t-1}2^k, k > 1, \text{ or if}$$

$$y = p_{t-1}2J, \text{ where } J \text{ is a single prime } \geq 3, \text{ or a product of primes } \geq 3, \text{ or if}$$

$$y = p_{t-1}K, \text{ where } K \text{ is a product of at least two odd primes,}$$

then again we have our q , namely, p'' .

So, if our desired q is not to exist, it must be the case that

$$y = p_{t-1}2 \text{ or}$$

$$y = p_{t-1}3.$$

But then z contains as factors all primes in P except p_t, p_{t-1} , and 2 or 3. But this is impossible, because if x is a prime, then, as Jonquières proved² in 1884, z must equal $y + 1$, and since there are more than 10,000 primes less than 125,000 (by the Prime Number Theorem³), z is far

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

2. *ibid.*, p. 64.

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

too large to equal $y + 1$.

Thus q exists. \square

3. This theorem asserts: if $\pi(x)$ denotes the number of primes that do not exceed x , then $\pi(x)$ is asymptotic to $x/(\log x)$.

Appendix F — Statement and Proof of Certain Numbered Statements and of Lemmas

(1.8): Statement and Proof

Exactly one of x, y, z must be even.

Proof:

By (1.5) (see under “Initial Assumptions, Definitions, and Properties of Numbers Involved” on page 9 of Part (1) of this paper, on the web site occampress.com), neither two or three of x, y, z contains the factor 2. If none of x, y, z contains the factor 2, then we have two odd integers summing to an odd integer, which is impossible. \square

(1.85): Statement and Proof

(1.85) *It suffices to prove FLT for every odd prime ≥ 3 .*

Proof:

Fermat himself proved FLT for the exponent 4. A number $n \geq 3$ that is not a multiple of 4 must be a multiple of an odd prime. Thus if $n = pK$, and we prove FLT for p , then we have proved it for $n = pK$ because we have proved that, for all x, y, z

$$x^p + y^p \neq z^p$$

hence for all u, v, w

$$(u^K)^p + (v^K)^p \neq (w^K)^p$$

or

$$u^n + v^n \neq w^n$$

\square

(1.90) (a)

If $a + b, c < m$, and $a + b = c$, then $a + b \equiv c \pmod{m}$.

(1.90) (b)

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

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

For inequalities:

(1.91) (a)

If $(a,m) = (b,m) = (c,m) = 1$, then if
 $a + b, c < m$, and
 $a + b \neq c$,
then $a + b$ is not $\equiv c \pmod m$.

(1.91) (b)

If $(a,m) = (b,m) = (c,m) = 1$, and if
 $a \equiv a' \pmod m$, and $b \equiv b' \pmod m$, and $c \equiv c' \pmod m$, then
if $a + b$ is not $\equiv c \pmod m$ then $a' + b'$ is not $\equiv c' \pmod m$.

Proof of (1.91) (b):

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

We prove the contrapositive of our statement.

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

(1.91) (c)

If $(a,m) = (b,m) = (c,m) = 1$, and if
 $a \equiv a' \pmod m$, and $b \equiv b' \pmod m$, and $c \equiv c' \pmod m$, then
if $a^r + b^r \equiv c^r \pmod m$, $r \geq 1$,
then $a^{r'} + b^{r'} \equiv c^{r'} \pmod m$ and
 $a^r \equiv a^{r'} \pmod m$ and $b^r \equiv b^{r'} \pmod m$ and $c^r \equiv c^{r'} \pmod m$.

Proof of (1.91) (c):

If $a \equiv a' \pmod m$, and $b \equiv b' \pmod m$, and $c \equiv c' \pmod m$, then, by definition of congruence, this implies that there exist integers h, j, k such that $a' = a + hm$, $b' = b + jm$ and $c' = c + km$. Therefore $a = a' - hm$, $b = b' - jm$ and $c = c' - km$, or, $a = a' + h'm$, $b = b' + j'm$ and $c = c' + k'm$.

Then $a^r + b^r \equiv c^r \pmod m$ implies $(a' + h'm)^r + (b' + j'm)^r \equiv (c' + k'm)^r \pmod m$.

By the binomial theorem, this yields:

$(a'^r + (Hm)) + (b'^r + (Jm)) \equiv (c'^r + (Km)) \pmod m$, or, since $m \equiv 0 \pmod m$,
 $a'^r + b'^r \equiv c'^r \pmod m$. \square

(1.91) (d)

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

\

In addition, we will need Fermat’s Little Theorem, which states:\

(1.92) (Fermat’s Little Theorem)

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

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

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

$$\begin{aligned} a^{(q-1)+1} &\equiv a \pmod{q}, \\ a^{(q-1)+2} &\equiv a^2 \pmod{q}, \\ a^{(q-1)+3} &\equiv a^3 \pmod{q}, \\ &\dots \end{aligned}$$

In other words, powers of a are congruent mod $(q - 1)$. Thus $(q - 1)$ is a modulus that defines a set of $(q - 1)$ congruence classes.

We will also need Euler’s generalization of Fermat’s Little Theorem:

(1.93)

If $(a, m) = 1$ then $a^{\phi(m)} \equiv 1 \pmod{m}$, where ϕ denotes Euler’s totient function. $\phi(m)$ is the number of numbers $n < m$ such that $(n, m) = 1$.

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

$$\begin{aligned} a^{\phi(m)} &\equiv 1 \pmod{m}, \\ a^{\phi(m)+1} &\equiv a \pmod{m} \\ a^{\phi(m)+2} &\equiv a^2 \pmod{m} \\ &\dots \\ a^{2\phi(m)} &\equiv a^{\phi(m)} \pmod{m} \\ &\dots \end{aligned}$$

In other words, powers of a are congruent mod $\phi(m)$. Thus $\phi(m)$ is a modulus that defines a set of $\phi(m)$ congruence classes.

(1.94)

If $a + b \equiv c \pmod{q^k}$, $k \geq 2$,
Then $a + b \equiv c \pmod{q^{k-j}}$, $1 \leq j < k$.

Proof of (1.94):

By definition of congruence, if $a + b \equiv c \pmod{q^k}$, $k \geq 2$, then there exists an $h \geq 1$ such that $a + b + hq^k = c$. But then $a + b + (hq^j)q^{k-j} = c$, hence $a + b \equiv c \pmod{q^{k-j}}$. \square

(1.95)

If $(k, m) = d$
Then the congruence $ka \equiv b \pmod{m}$ is soluble iff d divides b .

Proof of (1.95):

See any textbook on elementary congruence theory.

Lemma 0.0: Statement and Proof

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

Proof.

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

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

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

Lemma 0.2: Statement and Proof

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

- (a) $x + y - z = Kdef$, where $K \geq 1, d, e, f > 1$;
 - (b) $Kdef$ contains the factors 2 and p ;
 - (c) d is a factor of x ;
 e is a factor of y ;
 f is a factor of z ;
 - (d) $(d, e, f) = 1$;
 - (e) if $x^k + y^k - z^k \equiv 0 \pmod k$, where k is a prime, $3 \leq k < p$, then $Kdef$ contains a factor k .
- (e) $p < (1/30)(x)$. Thus, prior to Wiles’ proof of FLT, the smallest x in a counterexample was at least 3,750,000.

Proof of Lemma 0.2 (a):

See “Approach via Factors of x, y, z ” on page 44 of Part (1) of this paper, on the web site occampress.com.

Proof of Lemma 0.2 (b):

Since exactly one of x, y, z is a multiple of 2, the other two being odd, positive numbers, $x + y - z$ must be a multiple of 2.

A basic result¹ of congruence theory states:

If k is an odd prime, then $(a + b + c + \dots + g)^k \equiv a^k + b^k + c^k + \dots + g^k \pmod k$.

Let $a = x, b = y, c = -z$. Then we have:

$$(x + y - z)^k \equiv x^k + y^k - z^k \pmod k, \text{ where } 3 \leq k \leq p. \tag{1}$$

1. See, for example, Gauss’s *Disquisitiones Arithmeticae*, Article 51.

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

By assumption $x^p + y^p = z^p$, so $x^p + y^p - z^p = 0$ and hence, by (1),

$$(x + y - z)^p \equiv 0 \pmod{p}.$$

Since we know that $x + y - z \neq 0$ (“Lemma 0.0” on page 10 of Part (1) of this paper, on the web site occampress.com.), we conclude that $x + y - z$ is a non-zero multiple of p . \square

Proof of Lemma 0.2 (c):

See “Approach via Factors of x, y, z ” on page 44 of Part (1) of this paper, on the web site occampress.com.

Proof of Lemma 0.2 (d):

By the basic result cited in the proof of part (b), we know that

$$(x + y - z)^k \equiv x^k + y^k - z^k \pmod{k}, \text{ where } 3 \leq k \leq p.$$

By part (a), $(x + y - z) = Kdef$. Therefore

$$(x + y - z)^k = (Kdef)^k \equiv x^k + y^k - z^k \pmod{k}. \tag{1}$$

It is not possible, by our assumption that p is the smallest prime in a counterexample, that $x^k + y^k - z^k = 0$ if $3 \leq k < p$. Hence if $x^k + y^k - z^k \equiv 0 \pmod{k}$, it must be the case that $x^k + y^k - z^k$ is a non-zero multiple of k . The result follows from (1). \square

Proof of Lemma 0.2 (e):

By parts (a), (b), and (c) of this Lemma, $x + y - z = Kdef$, where K contains the factors 2 and p , $d, e, f > 1$, d, e, f are relatively prime, and d is a factor of x , e is a factor of y , and f is a factor of z . By part (b) of “Lemma 1.5.” on page 11 of Part (1) of this paper, on the web site occampress.com, $x + y - z < x$. Since d, e , and f are each greater than 1 and are relatively prime factors of x, y , and z , and since one of d, e, f might be the factor 2 in K , we have $Kdef \geq p(2)(3)(5) < x$, hence $p < (1/30)(x)$. Prior to Wiles’ proof it was known that p was greater than 125,000. Hence, the smallest value of x was at least 1,375,000. \square

Proof of Lemma 0.2 (f):

Follows directly, by definition of congruence, from parts (a) and (b).

Lemma 0.3: Lemma and Proof

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

Proof: The Lemma is a specific case of the basic result¹,

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

If k is an odd prime, then $(a + b + c + \dots + g)^k \equiv a^k + b^k + c^k + \dots + g^k \pmod k$. \square

Lemma 0.5: Statement and Proof

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

Proof:

1. Let $x^2 + y^2 = z^2$.
2. Raise both sides of this equation to the power $p/2$. We get:

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

Clearly, $x^p + y^p < z^p$. \square

Lemma 0.6: Statement and Proof

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

Proof:

If $x^n + y^n \neq z^n$ for all x, y, z , then certainly $(u^k)^n + (v^k)^n \neq (w^k)^n$, for all $u, v, w, k \geq 1$. \square

Lemma 1.0: Statement and Proof

- (a) $p < x < y < z$.
- (b) $z < x + y < 2y < 2z$.

Proof of Lemma 1.0 (a):

We quote from Ribenboim, Paulo, *13 Lectures on Fermat’s Last Theorem*, Springer-Verlag, N.Y., 1979, p. 226.

“In 1856, Grünert proved:

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

“Proof:

“ $x^n = z^n - y^n = (z - y)(z^{n-1} + z^{n-2}y + \dots + y^{n-1}) > (z - y)ny^{n-1}$.

“Hence

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

“and

1. See, for example, Gauss’s *Disquisitiones Arithmeticae*, Article 51.

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

“so $n < x$.” □

Proof of Lemma 1.0 (b):

$z < x + y$ by part (a) of Lemma 1.5, below;

$x + y < 2y$ by part (a) of this Lemma;

$2y < 2z$ by part (a) of this Lemma.. □

Lemma 1.5: Statement and Proof

Let x, y, z, p be elements of the minimum counterexample. Then for all $k, 1 \leq k < p$, k real and not merely integral:

(a) $x^k + y^k > z^k$, i.e., $x^k + y^k - z^k > 0$; ^{1, 2}

(b) $x^k + y^k - z^k < x^k$;

(c) $x^k + y^k$ increases monotonically with increasing k ;

(d) z^k increases monotonically with increasing k ;

(e) $(x^k + y^k)/z^k > (x^{k+1} + y^{k+1})/z^{k+1}$.

(f) Let $f(k) = x^k + y^k - z^k$. Then the slope of f , namely, $x^k(\ln x) + y^k(\ln y) - z^k(\ln z)$, is positive for all k , where $1 \leq k < p - 1$, k real and not merely integral. Thus $x^k + y^k - z^k < x^{k+1} + y^{k+1} - z^{k+1}$ for integral $k, 1 \leq k \leq p - 2$.

(g) $x^k + y^k - z^k \geq Kdef + k - 1$, where here k is integral and $Kdef$ are as defined in “Lemma 0.2” on page 10, of Part (1) of this paper, on the web site occampress.com. Hence, in particular, since the maximum of the function $x^k + y^k - z^k$ occurs at $p - 1 \leq k < p$, it has value $\geq Kdef + p - 2$.

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

Remark: Parts (b) and (g) imply that $Kdef + k - 1 \leq x^k + y^k - z^k < x^k$. This in turn implies that $x^k + y^k - z^k$ increases by 1 with each incremental increase in k , which is definitely surprising.

Note: The proofs of parts (a), (c), (d), and (e) are Ed Boyda’s improvements of our clumsy originals. Any errors in these proofs are due to our faulty transcriptions. The proof of part (f) is entirely Boyda’s, but, again, any errors are due to our faulty transcription.

Proof of Lemma 1.5 (a)

By assumption of a counterexample, $x^p + y^p = z^p$. Then since $z > x, y$, for a such that $p > a > 0$,

1. Students of the phenomenon of mathematical intuition might be interested to know that from the moment we realized that, if a counterexample $x^p + y^p = z^p$ exists, then $x + y$ must be greater than z , he was convinced this would be part of a “simple” proof of FLT if he was able to discover one. We have no explanation for his conviction, nor does he claim that his conviction will be vindicated.

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

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

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

$$x^{(p-a)} + y^{(p-a)} > z^{(p-a)}. \quad \square$$

Proof of Lemma 1.5 (b)

Assume, to the contrary, that $x^k + y^k - z^k \geq x^k$, $1 \leq k \leq p-1$. Then $y^k - z^k \geq 0$, which is a contradiction, since $y < z$ \square

Proof of Lemma 1.5 (c)

Follows directly from a known property of the exponentiation function, and the fact that x, y, k are positive integers, and x, y are fixed. \square

Proof of Lemma 1.5 (d)

Follows directly from a known property of the exponentiation function, and the fact that z, k are positive integers, and z is fixed. \square

Proof of Lemma 1.5 (e)

For a, b , such that $0 < a < b < p$:

$$\begin{aligned} (x^p + y^p)/z^p &< z^a (x^{(p-a)} + y^{(p-a)})/z^p = \\ (x^{(p-a)} + y^{(p-a)})/z^{(p-a)} &< \\ z^b (x^{(p-b)} + y^{(p-b)})/z^p &= \\ (x^{(p-b)} + y^{(p-b)})/z^{(p-b)}. &\quad \square \end{aligned}$$

Proof of Lemma 1.5 (f)

1. We begin by asserting that:

(1)

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

Proof:

1.1 We can rewrite (1) as:

(2)

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

1.2 By part (a) of this Lemma, we know that $x^{k+1} + y^{k+1} > z^{k+1}$ and thus we get the left-hand inequality of (2), hence of (1).

1.3 For all $u, v > e$ (the base of the natural logarithms), if $u < v$ then $(\ln u)/u > (\ln v)/v$.

Proof:

We show that, for all $w > e$, the base of the natural logarithms, the derivative of $(\ln w)/w$ is negative.

By the basic rule for the derivative of a fraction,

$$\frac{d\left(\frac{\ln w}{w}\right)}{dw} = \frac{w\left(\frac{d(\ln w)}{dw}\right) - (\ln w)\left(\frac{dw}{dw}\right)}{w^2} = \frac{w\left(\frac{1}{w}\right) - (\ln w)}{w^2} = \frac{1 - (\ln w)}{w^2}$$

The rightmost term is negative because the natural logarithm of all $w > 3$ is > 1 . \square

1.4 Therefore, since $e < y < z$, it follows that $(\ln y)/y > (\ln z)/z$, hence $z/y > (\ln z)/(\ln y)$, and we have the left-hand inequality and the right-hand inequality of (2), hence of (1). \square

2. In (1), cross-multiply z^k in the denominator of the left-hand term, with $\ln z$ in the numerator of the right-hand term, yielding $z^k (\ln z)$ in the numerator of the right-hand term.

In (1), cross-multiply $\ln y$ in the denominator of the right-hand term with the numerator of the left-hand term, yielding

$$(x^k)(x(\ln y)/y) + y^k (\ln y)$$

But since, by step 1.3, $y/x > \ln y/\ln x$, $\ln x > (x(\ln y))/y$, and so, from what we have established in this step, we can write

$$(x^k)(\ln x) + y^k (\ln y) > z^k (\ln z), \text{ which implies that}$$

$$(x^k)(\ln x) + y^k (\ln y) - z^k (\ln z) > 0, \text{ which is the desired result. } \square$$

Proof of Lemma 1.5 (g)

By part (f) of this Lemma, $x^k + y^k - z^k < x^{k+1} + y^{k+1} - z^{k+1}$ for all $k, 1 \leq k \leq p - 2$. Since, by “Lemma 0.2” on page 10 of Part (1) of this paper, on the web site occampress.com., $x + y - z =$

Kdef, the result follows. \square

Proof of Lemma 1.5 (h)

Since by “Lemma 1.0.” on page 11 of Part (1) of this paper, on the web site occampress.com. $x < y < z$, it must be that $x^k < y^k < x^k + y^k < 2y^k < 2z^k$. That $z^k < x^k + y^k$ is established by part (a) of this Lemma. \square

Lemma 1.95. Statement and Proof

Let x, y, z , be elements of the minimum counterexample $x^p + y^p = z^p$. Then for all $k > p$, $x^k + y^k < z^k$.

Proof of Lemma 1.95:

1. We use proof by induction.

Basis step

1. Assume that

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

2. Then

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

3. But then it must be the case that

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

Inductive step

4. Assume that for all $j, p < j \leq k$, $x^j + y^j < z^j$.

2. Then

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

3. But then it must certainly be the case that

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

We can establish more regarding the ratios

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

when $k > p = n + 1$ as will be seen in the next lemma.

Lemma 1.97¹: Statement and Proof

Let x, y, z , be elements of a counterexample $x^{(p=n+1)} + y^{(p=n+1)} = z^{(p=n+1)}$ to FLT, where $p = n + 1$ is the smallest such exponent. Then

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

First (and Simplest) Proof of Lemma 1.97:

1. By Lemma 1.0, $x < y < z$.
2. Therefore $(x/z)^k$ can be made arbitrarily small for sufficiently large k , and similarly for $(y/z)^k$. Thus

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

□

Second Proof of Lemma 1.97:

1. If we can prove that

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

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

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

1. A young mathematician has written us that Lemma 1.97 “bears a major resemblance to what is known as the ABC Conjecture, ... a long unsolved problem in additive number theory... The ABC Conjecture almost proves FLT in the sense that if ABC is true, then for all n sufficiently large, $x^n + y^n = z^n$ has no integer solutions. See for instance mathworld.wolfram.com/abcconjecture.html.”

y^k .

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

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

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

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

Etc. The result follows. \square

Remark on Second Proof

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

Lemma 2.0. Statement and Proof

$z < 2y$.

Proof of Lemma 2.0.

$x^n + y^n < 2y^n < (2y)^n$, so z cannot be $\geq 2y$. \square

Lemma 3.0. Statement and Proof

See “Appendix A — Lemma 3.0” on page 2.

Lemma 4.0. Statement and Proof

Assume a counterexample $x^p + y^p = z^p$ exists. Then p cannot be a member of a certain infinite set of primes.

Proof of Lemma 4.0

1. Assume a counterexample $x^p + y^p = z^p$ exists. By “Definition of “Minimum Counterexample”” on page 9 of Part (1) of this paper, on the web site occampress.com, p is the smallest such prime.

2. As proved under “Discussion” on page 58 of Part (1) of this paper, on the web site occampress.com, it is not possible that $x + y = z$.

3. Let q be a prime such that $(x, q) = (y, q) = (z, q) = 1$ and $x + y, z < q$. Such a prime must exist because there are an infinite number of primes and only a finite number of prime factors,

total, in x , y , and z .

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

$$(1.95) \quad x^{1+k(q-1)} + y^{1+k(q-1)} \text{ is not } \equiv z^{1+k(q-1)} \pmod{q},$$

where $k \geq 0$.

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

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

$$x + y \neq z$$

and the fact that there exists a prime q such that $x + y$ and z are both less than q , led to an infinity of facts, namely the non-congruences expressed by (1.95), which in turn gave us another infinity of facts, namely, that the prime p in the assumed counterexample could not be one of the infinity of primes required by Dirichlet’s Theorem.

A young mathematician stated and proved the following, stronger version of Lemma 4.0. (The proof given here is a slightly edited version of the original. Any errors are entirely our responsibility.)

Lemma 4.0.5: Statement and Proof

Assume a counterexample $x^p + y^p = z^p$ exists. Then p can be at most one prime.

First Proof of Lemma 4.0.5

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

1. Let us assume there are *two* primes $p < q$ for which:

$$\begin{aligned} x^p + y^p &= z^p; \\ x^q + y^q &= z^q. \end{aligned}$$

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

$$x^q + y^q = (x^p)^r + (y^p)^r < (x^p + y^p)^r = (z^p)^r = z^q = x^q + y^q,$$

which is a contradiction. Therefore there cannot be two p which yield counterexamples for given x , y , z . \square

Second Proof of Lemma 4.0.5:

“The Fermat curves $C_m: X^m + Y^m = 1$ intersect trivially.” (A reader) \square

Lemma 6.0. Statement and Proof

See “Appendix D — Proof of Lemma 6.0” on page 3.

Lemma 10.0: Statement and Proof

Let u, v, w each be less than m , and let $(u, m) = (v, m) = (w, m) = 1$. If for all j , where $1 \leq j \leq \varphi(m)$, $C_{u, v, w, j, m}$ is non-congruent, then $\langle x^p + y^p, z^p \rangle$ is not an element of the C -set.

Proof:

The exponent p must be congruent to a j in the range $1 \leq j \leq \varphi(m)$. But the element $\langle x^p + y^p, z^p \rangle$ must be congruent, whereas, by hypothesis each $C_{u, v, w, j, m}$ is non-congruent, and therefore can contain no counterexample element. \square

Lemma 12.0: Statement and Proof

Let q be an odd prime such that $(x, q) = (y, q) = (z, q) = 1$, and $x, y, z > q$ (see “Lemma 30.0: Statement and Proof” on page 18). Let $k \geq 1$. Let \mathbf{K} be the set of all C -sets mod q^k such that $1 \leq j \leq \varphi(q^k)$, where j is the exponent of terms in the base element. In other words, \mathbf{K} contains all C -sets mod q^k . Let \mathbf{K}' be the subset of \mathbf{K} consisting of all C -sets such that $1 \leq j \leq k$. Then each C -set in \mathbf{K}' is non-congruent.

Proof:

We know that if $x^j + y^j$ and z^j are each less than q^k then $x^j + y^j \neq z^j$. Hence the C -set of which $x^j + y^j$ and z^j constitute the base element must be a non-congruent C -set and can contain no counterexample element.

If $x^j + y^j \equiv z^j \pmod{q^k}$ then by definition of congruence, there exists an h such that $x^j + y^j + hq^k = z^j$, where $h \neq 0$. (It is not possible that $h = 0$ because we are assuming that p is greater than $\varphi(q^k)$ and all our j 's are less than $\varphi(q^k)$ (step 1).)

We know that $x^j + y^j > z^j$ and $x^j + y^j - z^j < x^j$ (see “Lemma 1.5.” on page 11 of Part (1) of this paper, on the web site occampress.com) so $z^j < x^j + y^j < z^j + x^j$. Thus the difference between z^j and $x^j + y^j$ is less than x^j . But by our assumption regarding q in step 1, $x^i < q^i$ for all $i \geq 1$. Therefore, in particular, $x^k < q^k$. And thus there does not exist an $h \neq 0$ such that $x^j + y^j + hq^k = z^j$. Thus (1) is proved.

Lemma 30.0: Statement and Proof

There exists a prime q , hence a smallest prime q , such that $(x, q) = (y, q) = (z, q) = 1$ and such that at least one of x, y, z is greater than q , and therefore such that our assumed minimum counterexample $x^p + y^p = z^p > q$.

We provide three proofs. In the first, we prove that the desired prime q is less than y , which, by “Lemma 1.0.” on page 11 of Part (1) of this paper, on the web site occampress.com, is less than z .

First Proof:

1. We know that x is the product of one or more primes. If there is a prime $q < x$ that is relatively prime to x , y , and z , then we are done: q is the desired modulus.

2. So assume that at least one prime less than x and relatively prime to x is a factor of y or z . A basic result of number theory states that each of the primes that are factors of y is less than or equal to \sqrt{y} . If we can prove that there is a prime q such that

(1)

$$\sqrt{y} < \sqrt{z} < q < 2 \cdot \sqrt{z} < y.$$

then we will have our desired q . For by Bertrand’s Postulate, which states that for all positive integers n , there exists a prime between n and $2n$, we know that there is a prime q between \sqrt{z} and $2 \cdot \sqrt{z}$ (we take the smallest integer greater than or equal to \sqrt{z} as the value of \sqrt{z} , since the Postulate is stated for integers only). Since $\sqrt{y} < \sqrt{z} < q$ we know that q cannot be a factor of either y or z .

3. We now must prove that $2 \cdot \sqrt{z} < y$. By part (b) of “Lemma 1.0.” on page 11 of Part (1) of this paper, on the web site occampress.com, we know that $z < 2y$. Therefore $z/2 < y$. So we must prove that $2 \cdot \sqrt{z} < z/2$, or that

(2)

$$4 \cdot \sqrt{z} < z.$$

It is easy to show that (2) is true for all $z > 16$. We must therefore show that no counterexample can exist if $z \leq 16$. Since, by part (a) of “Lemma 1.0.” on page 11 of Part (1) of this paper, on the web site occampress.com, $p < x < y < z$, we could easily test each possibility for a counterexample. But this is unnecessary, since long before Wiles’ proof it was known that $p > 125,000$.

Thus we have proved that (1) holds, and we have our result. \square

Second Proof:

1. “Lucas proved...in 1891: y, z have at least two prime factors.”¹ We assume this means that y, z each have at least two prime factors.

Let P denote all the primes $\leq z$. Let the primes in P be listed in order of increasing magnitude, and let them be designated $p_1 = 2, p_2 = 3, p_3 = 5, \dots, p_t =$ the largest prime in P . If all the

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

primes in x, y, z do not exhaust all the primes in P , then we have our q : it is simply the smallest prime in P that is not a factor of $x, y,$ or z .

2. Therefore we must assume that $x, y,$ and z contain all primes in P . If p_t is a factor in a product H of two or more primes p_j , where $2 \leq p_j \leq p_t$, then there exists a prime p' such that $p_t < p' < 2p_t$, by “Bertrand’s Postulate” on page 13 of Part (1) of this paper, on the web site occampress.com. Clearly, $p' < H$, since all primes are ≥ 2 .

Thus we have our q (namely p') if p_t is a factor in a product H . Therefore, we must assume that $p_t = x$. We now ask if p_{t-1} is a factor of y . By Bertrand’s Postulate, we know that $p_{t-1} < p_t < 2p_{t-1}$, and that therefore there is a prime p'' , $2p_{t-1} < p'' < 4p_{t-1}$. So if

$$y = p_{t-1}2^k, \quad k > 1, \text{ or if}$$

$$y = p_{t-1}2J, \text{ where } J \text{ is a single prime } \geq 3, \text{ or a product of primes } \geq 3, \text{ or if}$$

$$y = p_{t-1}K, \text{ where } K \text{ is a product of at least two odd primes,}$$

then again we have our q , namely, p'' .

So, if our desired q is not to exist, it must be the case that

$$y = p_{t-1}2 \text{ or}$$

$$y = p_{t-1}3.$$

But then z contains as factors all primes in P except p_t, p_{t-1} , and 2 or 3. But this is impossible, because if x is a prime, then, as Jonquières proved¹ in 1884, z must equal $y + 1$.

It was known, as of 1990, that the exponent p in a counterexample must be greater than about 125,000. By “Lemma 1.0.” on page 11 of Part (1) of this paper, on the web site occampress.com, we know that $p < x < y < z$.

Since by the Prime Number Theorem² there are more than 10,000 primes less than 125,000, and all of these must be factors of z by step 3, it is clear that z is far too large to equal $y + 1$. Thus q exists. \square

Third Proof:

The above proof uses several results that were almost certainly unknown to Fermat. The question arises, Is there a proof of the Lemma that requires fewer of these results? The following proof requires only Bertrand’s Postulate and “Lemma 1.0.” on page 11 of Part (1) of this paper, on the web site occampress.com, which states that $p < x < y < z$. The Postulate was only proved in the 19th century (by Tschebyschef)³ and requires a quite sophisticated argument. So the proof was probably unknown to Fermat. On the other hand he might have assumed the Postulate was true based on his own empirical results. (Bertrand verified the Postulate for $n = 2$ to $n = 6,000,000$ before it was proved for all n .⁴)

1. *ibid.*, p. 64.

2. This theorem asserts: if $\pi(x)$ denotes the number of primes that do not exceed x , then $\pi(x)$ is asymptotic to $x/(\log x)$.

3. Niven, Ivan, and Zuckerman, H. S., *An Introduction to The Theory of Numbers*, Fourth Edition, John Wiley & Sons, N.Y., 1972, p. 224.

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

Lemma 1.0 is easy to prove, as the reader can see by looking at the proof in this Appendix, so we can reasonably assume that Fermat had a proof if in fact he used this Lemma.

1. Let P = the set of all primes that are factors of x , y , and z and assume that P consists of the first t primes, where $t \geq 1$. Furthermore assume that P contains all primes $\leq z$. (Otherwise, if P did not contain one or more primes $\leq z$, the least of these would be our desired prime q .) Let the primes in P be designated $p_1 = 2, p_2 = 3, p_3 = 5, \dots, p_t =$ the largest prime in P .

2. “Lemma 45.0: Statement and Proof” on page 23 states:

Let n be a positive integer greater than 1. Then there are at least k primes between n and $2^k n$, where $k \geq 1$.

It follows that neither x, y , nor z can contain the product Up_t , where U is a product of primes in P . For, suppose w contained such a product, where w is x, y , or z . Then by Lemma 45.0 there would be a prime between p_t and w , contrary to the definition of P and p_t .

Furthermore it follows that neither x, y , nor z can contain the product $U'p_{t-1}$, where U' is a product of primes in P whose value $\geq 2^2$. For, suppose w contained such a product, where w is x, y , or z . Then by Lemma 45.0 there would be two primes between p_{t-1} and w . One of these would be p_t . The second would contradict the definition of P and p_t .

Finally, it follows that neither x, y , nor z can contain the product $U''p_{t-2}$, where U'' is a product of primes in P whose value $\geq 2^3$. The reason is similar to that for the previous two cases.

3. By “Lemma 1.5.” on page 11 of Part (1) of this paper, on the web site occampress.com- which asserts that $(x, y) = (y, z) = (x, z) = 1$, we have that:

one of $x, y, z = p_{t-2}$ or $2p_{t-2}$ or $3p_{t-2}$ or 2^2p_{t-2} or $6p_{t-2}$.
another of $x, y, z = p_{t-1}$ or $2p_{t-1}$ or $3p_{t-1}$;
the third of $x, y, z = p_t$;

By definition of P , then, $P = \{2, 3, 5, 7\}$, where

$p_{t-3} = 2$ (a 2 factor is required by (1.8): see “(1.8): Statement and Proof” on page 5);
 $p_{t-2} = 3$;
 $p_{t-1} = 5$;
 $p_t = 7$.

4. We can therefore write, for possible values of x, y , and z , with no suggestion being made here as to which values apply to which of x, y, z :

4. *ibid.*, p. 224.

(1)

2, 2^2 , 2^3 ; (2^4 is not a candidate because there is a q , namely 11 or 13, that is less than 2^4);

3, 6, 9, 12, 18;

5, 10, 15;

7

5. We could now make a table of all legitimate assignments of the numbers in (1) to x , y , z and show that for each of these, there is a prime q meeting the requirements of the Lemma. The reader can determine for him- or herself that most of the possible assignments will be illegitimate. For example, since, by “Lemma 0.0” on page 10 of Part (1) of this paper, on the web site occam-press.com, in a counterexample, $x + y > z$, the following are all illegitimate assignments:

Table 1:

x candidate	y candidate	z candidate
2	3	5
3	4	7
4	5	9
5	9	14

So are all assignments in which $x + y < z$, such as:

x candidate	y candidate	z candidate
2	3	7
5	7	18

Unfortunately, there is at least one assignment, namely, $x = 7$, $y = 9$ and $z = 10$, that is legitimate but does not give us the desired q . But this, and all assignments having the same property, do not constitute an obstacle, since Lemma 1.0 guarantees us that $p < x < y < z$ and so in these cases we can simply compute $x^p + y^p$ and z^p and see if inequality holds. It does in all cases¹. (For example, $7^5 + 9^5 \neq 10^5$, and similarly $7^3 + 9^3 \neq 10^3$.)

Among legitimate assignments, for example: $x = 4$, $y = 5$, and $z = 7$ yields 3 as our desired q ; x

1. All these cases could easily have been checked by Fermat. In passing, we mention that by 1850, thanks to the efforts of E. E. Kummer, FLT was known to be true for all primes less than 100 except for 37, 59, and 67. — Ribenboim, op. cit., p 9.

= 4, $y = 7$, and $z = 9$ yields 5 as our desired q .

And so we have our result. \square

Lemma 45.0: Statement and Proof

Let n be a positive integer greater than 1. Then there are at least k primes between n and $2^k n$, where $k \geq 1$.

Proof:

Follows directly “Bertrand’s Postulate” on page 13 of Part (1) of this paper, on the web site occampress.com, which states that if n is a positive integer, then there is at least one prime between n and $2n$. Hence there is at least one prime between $2n$ and $4n$, and at least one prime between $4n$ and $8n$, etc. \square

Lemma 50.0: Statement and Proof

Let $1 < a < b$, where a, b are integers and $(a, b) = 1$. Let p be an odd prime, and let $(a, p) = (b, p) = 1$. Let the largest power of p that divides $a + b$ be p^k , where $k \geq 1$. By the binomial theorem we know that $(a + b)^p = a^p + H + b^p$. Then p^{k+1} , but no larger power of p , divides H .

Proof:

The following proof is a slightly-edited version of a proof by a mathematics graduate student. All errors are entirely our own.

1. Let $a + b = p^k M$, where $(M, p) = 1$. Then $b = p^k M - a$.

2. By the binomial theorem

$$b^p = (p^k M - a)^p = ((-a) + p^k M)^p = (-a)^p + p(-a)^{p-1} p^k M + (p(p-1)/2)((-a)^{p-2} p^{2k} M^2 + \dots) \quad (1)$$

3. The third term on the right-hand side of (1) is divisible by p^{2k+1} and therefore, since $k \geq 1$, by p^{k+2} . Furthermore, each term in the ellipsis, “...”, is divisible by p^{3k} and hence by p^{k+2} .

Thus

$$b^p = (-a)^p + (-a)^{p-1} p^{k+1} M + p^{k+2} N, \text{ for some integer } N.$$

It follows that

$$b^p + a^p = (-a)^{p-1} p^{k+1} M + p^{k+2} N,$$

and we have

$$(a + b)^p - a^p - b^p = p^{pk} M^p - (-a)^{p-1} p^{k+1} M - p^{k+2} N. \quad (2)$$

4. Each term on the right-hand side of (2) is divisible by p^{k+1} . The first term is divisible by p^{k+2} (since $p \geq 3$ and $k \geq 1$) and the last term is divisible by p^{k+2} . However, the middle term is not divisible by p^{k+2} (since p does not divide a or M). Thus, p^{k+2} does not divide $H = (a + b)^p - a^p - b^p$. \square

Lemma 55.0: Statement and Proof

Let $1 < a < b$, where a, b are integers and $(a, b) = 1$. Let p be an odd prime, and let $(a, p) = (b, p) = 1$. Let the largest power of a prime q , where $q \neq p$, that divides $a + b$ be q^k , where $k \geq 1$. By the binomial theorem we know that $(a + b)^p = a^p + H + b^p$. Then q^k , but no larger power of q , divides H .

Proof:

The following proof is a slightly-edited version of a proof by a mathematics graduate student. All errors are entirely our own.

$$\begin{aligned} 1. \text{ Let } a + b = cq^k, \text{ where } (c, q) = 1. \text{ Then } (a + b)^p - a^p - b^p &= H = (cq^k)^p - a^p - (cq^k - a)^p \\ &= (cq^k)^p - a^p - (cq^k)^p + a^p + \sum_{i=1}^{p-1} \binom{p}{i} (-1)^{p-i+1} a^{p-i} (cq^k)^i = \\ &= \sum_{i=1}^{p-1} \binom{p}{i} (-1)^{p-i+1} a^{p-i} (cq^k)^i. \end{aligned}$$

2. The largest power of q that divides the $i = 1$ term in the above summation is k , since q does not divide any of the other factors in the term. The largest power of q that divides each of the other terms in the summation is greater than q^k , since the exponents in those terms are integral multiples of k . Therefore the largest power of q that divides H is q^k . \square

Lemma 60.0: Statement and Proof

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

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

One is via Fermat’s Little Theorem (see Part (4) of this paper), which implies that if

$$\begin{aligned} r &\equiv k \pmod{q-1}, \\ \text{then } x^r &\equiv x^k, y^r \equiv y^k, z^r \equiv z^k \pmod{q}. \end{aligned}$$

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

The other is via (1.91)(c) in Part (4) of this paper, which implies that if

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

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

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

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

Then:

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

(b) for each prime q , there is exactly one residue class mod q that contains no $U(k, a, b, c)$.

(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 , must be greater than q .

Proof:

Part (a)

1. By assumption of a counterexample, $U(p, x, y, z) = 0$. It follows that for each triple $\langle a^r, b^r, c^r \rangle$ that is congruent to the triple $\langle x^k, y^k, z^k \rangle$, $U(r, a, b, c)$ must be congruent to $U(p, x, y, z)$. Since $U(p, x, y, z) = 0$, it follows, by a basic fact of elementary congruence theory, that $U(r, a, b, c)$ is a multiple of q .

Part (b)

There are $q - 1$ sets S_k , hence $q - 1$ sets containing all $U(r, a, b, c)$. There are q residue classes mod q . The result follows. \square

Part (c)

Let $q = 2$. Then $q - 1 = 1$ and our set of exponents is $p \pm j$, where j is a positive integer such that $p - j$ is not negative. Then by part (a), each $U(k, a, b, c)$ is a multiple of 2. But since our set of exponents is all exponents such that $p - j$ is not negative, there cannot be any other $U(k, a, b, c)$, and so we have our result. \square

Part (d)

Seeking a contradiction, assume that both a^k and b^k , are less than or equal to q . Then since c^k is greater than or equal to 1, $a^k + b^k - c^k$ is less than $2q$, contradicting part (c). \square