

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

Part (3) Failed Implementations of Some Ideas 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

May 4, 2010

Key words: Fermat's Last Theorem

Introduction

In this Part, we collect descriptions of failed attempts at a proof of FLT that are based on some of the ideas in Part (1) of our paper (web site occampress.com). We collect these descriptions because we believe that there are readers who would like a clear, concise description of some of the difficulties we have run into.

For each attempt, we first give the argument (“Faulty Argument”), then we point out some of the errors (“Discussion”).

Attempt to Use Fermat’s Little Theorem

The following is one of the attempts discussed under “Original Motivation for Approaches via The “Lines-and-Circles” Model of Congruence” in Part (4) of this paper.

Faulty Argument

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

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

Discussion

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

Attempt to Apply the “Pushing-Away” (“Pushing-Up”) Strategy

This strategy is discussed in “Original Motivation for Approaches via The “Lines-and-Circles” Model of Congruence” and in subsequent sections.

Faulty Argument

1. Assume $x^p + y^p = z^p$ is a minimum counterexample. By Lemma 4.0.5, Lemma 0.0, and Lemma 0.2, we know that for all positive integers k other than p , $x^k + y^k \neq z^k$. Therefore, for all such k , there exists a non-zero integer u_k such that $x^k + y^k - z^k = u_k$. Furthermore, we know by Lemma 1.5 that $u_k < x^k$.

2. Let q be the smallest prime greater than $x + y$, hence (by Lemma 0.0) greater than z . Then, clearly, $(x, q) = (y, q) = (z, q) = 1$. Furthermore, since $u_1 < x^1$, u_1 is not a multiple of q , so $x^1 + y^1$ is not $\equiv z^1 \pmod{q}$.

3. Now for all $k \geq 1$, if $x + y < q$, then $x^k + y^k < q^k$. (Proof: if $x + y < q$, then $(x + y)^k < q^k$. But by the binomial theorem, $(x + y)^k = x^k + U + y^k$, where U is positive. So $x^k + y^k < (x + y)^k < q^k$.)

Since $q^2 > z^2$, $(x, q^2) = (y, q^2) = (z, q^2) = 1$ and since $u_2 < x^2$, u_2 is not a multiple of q^2 , so $x^2 + y^2$ is not $\equiv z^2 \pmod{q^2}$.

...

3. We proceed in this manner up to and including the modulus q^p , at which point the counterexample $x^p + y^p = z^p$ “touches down” (is first less than a modulus, here q^p). But since each pair $\langle x^k + y^k, z^k \rangle$, $1 \leq k < p$, is a non-congruent base element of a necessarily non-congruent C-set, it follows that

the element $\langle x^p + y^p, z^p \rangle$, a congruent pair, must be in one of those C-sets, hence we have a contradiction and a proof of FLT.

Discussion

The error lies in the assumption that $\langle x^p + y^p, z^p \rangle$ must be an element of a C-set having $\langle x^k + y^k, z^k \rangle$ as base element. Since each C-set mod m is constructed using Fermat’s Little Theorem, elements $\langle x^i + y^i, z^i \rangle$ such that $i \not\equiv j \pmod{\phi(m)}$ are not in any C-set mod m . Thus if the counterexample element is one of these $\langle x^i + y^i, z^i \rangle$, the “pushing-away” strategy cannot work — there are no elements below the counterexample element in any C-set. In the case of our moduli $m = q^k$, $\phi(q^k) = q^{k-1}(q-1)$. But since $p < x < q$, the element $\langle x^p + y^p, z^p \rangle$ cannot be in any C-set having $\langle x^k + y^k, z^k \rangle$ as base element if $1 \leq k < p$.

Attempt to Use Relationship Between $x + y$ and z

Faulty Argument

1. Assume a counterexample $x^p + y^p = z^p$ exists, where $(x, y) = (y, z) = (x, z) = 1$. By part (a) of “Lemma 0.2” on page 10, we know that

$$x + y = z + pR, \tag{1}$$

where pR is positive and contains a prime factor q that is also a factor of z .

2. By the binomial theorem, from (1) we have

$$(x + y)^p = x^p + pK + y^p = (z + pR)^p = z^p + pL + (pR)^p. \tag{2}$$

By assumption of a counterexample, we have, from (2)

$$pK = pL + (pR)^p. \tag{3}$$

3. Divide through (3) by p . Now since, by step 1, q is a factor of z and of pR , it follows from the binomial theorem that L in the right-hand side of (3) contains a factor q . Therefore the right-hand side contains a factor q .

But since, by step 1, $(x, y) = (y, z) = (x, z)$, the left-hand side of (3) does not contain a factor q . This contradiction gives us a proof of FLT.

Discussion

The error lies in assuming that a sum of products each of which does not contain a prime q , cannot itself contain a factor q . The error can be seen immediately using congruences. We have:

$$\begin{aligned} x + y &= z + pR, \text{ where both } z \text{ and } pR \text{ contain a prime factor } q. \text{ Therefore} \\ x + y &\equiv 0 \pmod{q}. \\ z &\equiv 0 \pmod{q}, \text{ hence} \\ x + y &\equiv z \pmod{q}. \end{aligned}$$

Hence, by the binomial theorem,

$$(x + y)^p = x^p + pK + y^p \equiv z^p \pmod{q}.$$

By assumption of a counterexample, this yields

$$pK \equiv 0 \pmod{q}.$$

Attempt to Use Congruences Based on Assumed Counterexample

Consider a C-set having $\langle x^p + y^p, z^p \rangle$ as base element mod q , where q is an odd prime. Such a C-set has an infinity of elements $a^p + b^p \equiv c^p \pmod{q}$ where $a = x + dq$, $b = y + eq$, and $c = z + fq$. We are free to choose the integers d , e , and f as we please, although all must be positive, since x , y , z are each less than q , and we are dealing only with positive integers. So let us choose $d = x$, $e = y$, $f = z$. Then we have:

$$(x + xq)^p + (y + yq)^p + mq = (z + zq)^p$$

or, factoring,

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

which we can write as

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

Dividing through by $(1 + q)^p$ yields

$$x^p + y^p + \frac{mq}{(1+q)^p} = z^p$$

But since by assumption, $x^p + y^p = z^p$, this implies

$$\frac{mq}{(1+q)^p} = 0$$

which seems to be a contradiction, but which is not, since it simply implies that $m = 0$, which follows from the fact that if $x^p + y^p = z^p$, then $x^p(1+q^2)^p + y^p(1+q^2)^p = z^p(1+q^2)^p$.

Attempt (1) Based on Manipulation of Inequalities

By part (a) of “Lemma 1.5.” on page 11 of Part (1) of this paper we know that

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

It certainly follows that

$$x \cdot x^{p-1} + x \cdot y^{p-1} > x \cdot z^{p-1}$$

And it certainly follows that

$$x^p + y^p > x \cdot z^{p-1}$$

We ask now if it is possible that

$$x^p + y^p = x \cdot z^{p-1} + (z-x)z^{p-1} = z^p? \text{ The answer is yes, hence we have no contradiction.}$$

Attempt (2) Based on Manipulation of Inequalities

In Approach of Adding Inequalities, sub-section “Second Implementation of Approach”, we have (3) = (1), that is

(3) in “Second Implementation..”

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

(1) in “Second Implementation”

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

Multiplying through by $(x - 1)(y - 1)(z - 1)$, we get:

(1) in this Attempt

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

(2) in this Attempt

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

It is clear that the first, second, and third terms of (1) are less than the first, second, and third terms, respectively, of (2). That does not quite give us the inequality we need, however, since the last term is preceded by a minus sign. Can this potential obstacle be overcome? Let us move (1) over to (2)’s side of the equation expressed by (1) and (2), and get

(3)

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

or

(4)

$$(x - 1)(y - 1)((x^p - 1) + (y^p - 1) - (z^p - 2)) = 0$$

or, given our assumption that a counterexample exists, and hence that $x^p + y^p - z^p = 0$,

$$(x - 1)(y - 1)(0) = 0$$

which is not a contradiction.

Attempt to Use the Vector Inner Product

The following is an early version of the approach discussed under “Fifth Approach Using Inner Products”.

Faulty Argument

1. As we stated in the “Second Approach Using Inner Products”, the ordered triples $\langle x, y, -z \rangle$, and $\langle x^k, y^k, z^k \rangle$ where $1 \leq k \leq p - 1$ can each be regarded as a vector in 3-dimensional space.

2. Assume a counterexample exists. Then the inner product $\langle x, y, -z \rangle \bullet \langle x^{p-1}, y^{p-1}, z^{p-1} \rangle = x^p + y^p - z^p = 0$. By a basic fact of linear algebra, this implies that the angle between the two vectors is 90 degrees.

3. It follows that, for each j , $1 \leq j \leq p - 1$, there is a pair of vectors $\langle x^j, y^j, -z^j \rangle$, $\langle x^{p-j}, y^{p-j}, z^{p-j} \rangle$ that are at an angle of 90 degrees to each other. But this is impossible within one octant. Hence FLT is proved.

Discussion

The error lies in the claim that the vectors $\langle x^j, y^j, -z^j \rangle$, $\langle x^{p-j}, y^{p-j}, z^{p-j} \rangle$ are both in one octant. In fact, $\langle x^j, y^j, -z^j \rangle$ lies in the octant $\langle +, +, - \rangle$ whereas the vector $\langle x^{p-j}, y^{p-j}, z^{p-j} \rangle$ lies in the octant $\langle +, +, + \rangle$. A right angle can exist between two such vectors.

Attempt at a Continuity Argument

Faulty Argument

1. Seeking a contradiction, assume that a counterexample $x^p + y^p - z^p$ exists, and without loss of generality, assume it is a minimum counterexample. By part (a) of Lemma 1.5, we know that

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

is greater than 0. Call the value of this expression T .

2. By part (a) of Lemma 1.0, we know that $x < y < z$. If we multiply through (1) by x , we get a value U that is greater than T .

If we multiply through (1) by y , we get a value V that is greater than U , hence greater than T .

Finally, if we multiply through (1) by z , we get a value W that is greater than V , hence greater than U and hence greater than T .

3. Now let u increase continuously and monotonically, say linearly, from $u = x$ to $u = z$. For each value of u , we multiply through equation (1). Then if the value of u times (1) is, say, R , then the value of $(u + \Delta u)$ times (1), where Δu is an arbitrarily small, but positive, increase in u , will be greater than R .

4. Consider now (1) multiplied through by $u = z$. The value S must be positive. If we decrease the z that multiplies the x term until it is x , and if we decrease the z that multiplies the y term until it is y , we are decreasing the value of S . By assumption of a counterexample, we should have the resulting value 0. But this is not possible, given the monotonically increasing values of (1) as a result of multiplication by u .

Discussion

The error lies in assuming that two continuous functions having the same starting and ending values, must have the same intermediate values. The two functions in our case are (A) (1) multiplied through by u for all u in the range $x \leq u \leq z$, and (B) (1) with continuous, but independent increments in the values of x^{p-1} , y^{p-1} and z^{p-1} .