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@gmail.com
Phone: (510) 548-3827

July 13, 2013

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 Basic Factoring

Faulty Argument 1

Assume a counterexample $x^p + y^p = z^p$ exists, where (without loss of generality) x, y, z are relatively prime in pairs, $x < y < z$, and p is a prime. We assume that the counterexample is a minimum counterexample (see Part (1) of this paper, on occampress.com). But then we can write

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

Now if both z, y are not perfect squares, then $z^{p/2}$ and $y^{p/2}$ are each irrational, and if the sum and difference of two different irrational numbers is irrational, and if the product of two different irrational numbers is irrational, then we have our proof, because the left-hand side of (1) is irrational, whereas the right-hand side is rational.

In attempting to prove that both z, y are not perfect squares, we can assume that, to the contrary, they are: say $z = u^2$ and $y = v^2$. Then we have $(u^2)^p - (v^2)^p = x^p$, hence $(u^p - v^p)(u^p + v^p) = x^p$. Now $u^p - v^p$ cannot equal s^p for some s, because then we would have another counterexample, namely, $u^p - v^p = s^p$ or $v^p + s^p = u^p$, and since $u < z$, the counterexample would be a smaller one than our minimum counterexample. Furthermore, $u^p + v^p$ cannot equal t^p for some t, because then we would have another counterexample, namely, $u^p + v^p = t^p$, but since $v < y$, the counterexample would be a smaller one than our minimum counterexample. It is tempting to say that these two facts prove that z, y are not perfect squares. However, this would not be correct unless $(u^p - v^p)$ and $(u^p + v^p)$ can be shown to be relatively prime. On the other hand, the literature might already contain the result that z, y are not perfect squares.

Here is an attempt at proving that $(u^p - v^p)$ and $(u^p + v^p)$ are relatively prime. Assume the contrary. Then there exists a $k > 1$ such that $(u^p - v^p) = kU$, and $(u^p + v^p) = kV$. Adding the two equations yields $2u^p = k(U + V)$. Subtracting the first equation from the second yields $2v^p = k(V - U)$. We ask if k can be a multiple of 2. The answer is no, because then we would have $u^p = (k/2)(U + V)$ and $v^p = (k/2)(V - U)$, which implies that u, v have a factor in common, namely, $k/2$. But this is impossible since $u^2 = z$ *and* $v^2 = y$ and by assumption x, y, z are relatively prime in pairs. So $(U + V)$ *and* $(V - U)$ must each be divisible by 2. But then we would have $u^p = k((U + V)/2)$ and $v^p = k((V - U)/2)$, which again implies that u, v have a factor in common, namely, k, which is impossible since $u^2 = z$ and $v^2 = y$ and by assumption x, y, z are relatively prime in pairs. If our reasoning is correct, we have proved that $(u^p - v^p)$ and $(u^p + v^p)$ are relatively prime, which implies that z, y are not perfect squares. That in turn implies that $x^{p/2}$ and $y^{p/2}$ are each irrational, which implies what we have stated in the paragraph immediately following (1) above.

Discussion

It is not true in general that the product of two different irrationals is an irrational. Consider,

for example $(\sqrt{3} + \sqrt{2})(\sqrt{3} - \sqrt{2})$. The value is $3 - 2 = 1$. Furthermore, even though, by assumption, $(z^{p/2} + y^{p/2})(z^{p/2} - y^{p/2}) = z^p - y^p = x^p$, we cannot infer that $(z^{p/2} + y^{p/2})$ and $(z^{p/2} - y^{p/2})$ have prime factors. For example, although $(\sqrt{26} + \sqrt{2})(\sqrt{26} - \sqrt{2}) = 26 - 2 = 24$, we cannot infer that either factor contains 2, or 3. The reason is that the presence of irrational square roots takes us out of the domain of the integers, in which every integer has a unique factorization into prime powers, and into the domain of the reals, where this is not necessarily the case.

However, it is possible that our proof that z, y cannot be squares is valid.

Faulty Argument 2

1. By basic algebra, since p is a prime greater than 2, hence odd, we have that $(x + y)$ divides $(x^p + y^p)$. Since, by assumption of a counterexample, $x^p + y^p = z^p$, this implies $x + y$ divides z^p.

2. By Lemma 0.0 in Part (1) of this paper, on occampress.com, we know that $x + y > z$. By part (a) of Lemma 1.0 of this paper, on occampress.com, $x < y < z$. Thus it follows that $(x + y) < 2z$.

3. Now since $x + y$ divides z^p we know that each prime factor of $x + y$ must be a prime factor of z. (Of course, z may have other prime factors. Let M denote the set of these. It may be empty.)

4. We now ask how it is possible for $z < x + y < 2z$. From step 3, we claim that the power of at least one prime factor q of $x + y$ must be larger than the power of q in z. For if the power of each prime factor r of $x + y \leq$ the power of r in z, then $x + y \leq z$, contrary to step 2. (

The worst case for our purposes is that q is 2 and that the power of q in $x + y$ is 2 times the power of q in z. But this implies that $x + y \geq 2z$, whereas step 2 states that $x + y < 2z$. If this contradiction is valid, then we have a proof of FLT.

Discussion

The last paragraph is wrong. For example, consider

$z = 3^2 \bullet 5$;

$x + y = 3 \bullet 5^2$;

$2z = 2 \bullet 3^2 \bullet 5$.

We see that $x + y$ and z fulfill the conditions up to the last paragraph. And yet $x + y < 2z$, as required in step 2.

(I am indebted to a graduate student for pointing out the error in Faulty Argument 2.)

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 $x + y > z$. There-

fore $x + y$ not $\equiv z \bmod p$.

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

Discussion

First, Fermat's Little Theorem requires that $(x, p) = (y, p) = (z, p) = 1$, whereas it is entirely possible that one of x, y, z contains a factor p (see, e.g., Ribenboim, Paulo, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, N.Y., 1979, pp. 3-4).

If $x^p + y^p = z^p$, then not only is $x + y > z$, that is, $x + y = z + d$, where d is a positive integer, but d must contain a factor p (parts (a) and (b) of "Lemma 0.2: Statement and Proof" in Part (2) of this paper on occampress.com). We then have $x + y \equiv z \bmod p$, hence, by Fermat's Little Theorem, $x^p + y^p \equiv z^p \bmod p$ This means that there exists an integer r such that $x^p + y^p + rp = z^p$. If $r \neq 0$, then we have no counterexample. But if $r = 0$, we do, and at this elementary level, there is no way of knowing which case holds.

A more promising attempt to use Fermat's Little Theorem is given in Appendices A and B in Part (4) of this paper on occampress.com

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 $\equiv z^1 \bmod q$.

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 $\equiv z^2 \bmod q^2$.

...

3. We proceed in this manner up to and including the modulus q^p, at which point the counter-

example $x^p + y^p = z^p$ "touches down" (is first less than a modulus, here q^p). But since each pair $<x^k + y^k, z^k>$, $1 \le k < p$, is a non-congruent base element of a necessarily non-congruent **C**-set, it follows that
the element $<x^p + y^p, z^p>$, 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 $<x^p + y^p, z^p>$ must be an element of a **C**-set having $<x^k + y^k, z^k>$ as base element. Since each **C**-set mod m is constructed using Fermat's Little Theorem, elements $<x^i + y^i, z^i>$ such that i not $\equiv j$ mod $\varphi(m)$ are not in any **C**-set mod m. Thus if the counterexample element is one of these $<x^i + y^i, z^i>$, the "pushing-away" strategy cannot work — there are no elements below the counterexample element in any **C**-set. In the case of our moduli $m = q^k$, $\varphi(q^k) = q^{k-1}(q-1)$. But since $p < x < q$, the element $<x^p + y^p, z^p>$ cannot be in any **C**-set having $<x^k + y^k, z^k>$ as base element if $1 \le k < p$.

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

First 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 in Part (1) of this paper, on occampress.com, 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:

$x + y = z + pR$, where both z and pR contain a prime factor q. Therefore

$x + y \equiv 0 \bmod q$.
$z \equiv 0 \bmod q$, hence
$x + y \equiv z \bmod q$.

Hence, by the binomial theorem,

$(x + y)^p = x^p + pK + y^p \equiv z^p \bmod q$.

By assumption of a counterexample, this yields

$pK \equiv 0 \bmod q$.

Second Faulty Argument

1. By basic algebra, since p is a prime greater than 2, hence odd, we have that $(x + y)$ divides $(x^p + y^p)$. Since, by assumption of a counterexample, $x^p + y^p = z^p$, this implies $x + y$ divides z^p.

2. By Lemma 0.0 in Part (1) of this paper, on occampress.com, we know that $x + y > z$. By part (a) of Lemma 1.0 in Part (1), $x < y < z$. Thus it follows that $(x + y) < 2z$.

3. Now since $x + y$ divides z^p we know that each prime factor of $x + y$ must be a prime factor of z. (Of course, z may have other prime factors. Let M denote the set of these. It may be empty.) We do not make any claims about the powers of the prime factors in $x + y$ and z.

4. We now ask how it is possible for $z < x + y < 2z$. From step 3, we claim that the power of at least one prime factor q of $x + y$ must be larger than the power of q in z. The worst case for our purposes is that q is only 2 and that the power of q in $x + y$ is 2 times the power of q in z. But this implies that $x + y \geq 2z$, whereas step 2 states that $x + y < 2z$. If this contradiction is valid, then we have a proof of FLT.

Discusion

The following is derived from an email from a graduate student.
The implication in step 4, that $x + y \geq 2z$, is not valid. For assume:

$z = (3^2)(5) = 45$, so $2z = 90$;
$x + y = (3)(5^2) = 75$;

Here we have $z < x + y < 2z$, and each prime factor of $x + y$ divides z, hence divides z^p. Also, the power of 5 in $x + y$ is larger than it is in z. But the power of 3 in z is larger than in $x + y$, so we have $x + y$ is $(5/3)z$, which is less than 2z.

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 $a^p + b^p \equiv c^p \bmod q$ 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 in Part (1) of this paper we know that

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

It certainly follows that

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

And it certainly follows that

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

We ask now if it is possible that

$x^p + y^p = x \bullet z^{p-1} + (z-x)z^{p-1} = z^p$? 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 $<x, y, -z>$, and $<x^k, y^k, z^k>$ where $1 \le k \le p - 1$ can each be regarded as a vector in 3-dimensional space.

2. Assume a counterexample exists. Then the inner product $<x, y, -z> \bullet <x^{p-1}, y^{p-1}, z^{p-1}> = x^p + y^p - z^p = 0$. 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, $1 \le j \le p - 1$, there is a pair of vectors $<x^j, y^j, -z^j>$, $<x^{p-j}, y^{p-j}, z^{p-j}>$ 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 $<x^j, y^j, -z^j>$, $<x^{p-j}, y^{p-j}, z^{p-j}>$ are both in one octant. In fact, $<x^j, y^j, -z^j>$ lies in the octant <+, +, – > whereas the vector $<x^{p-j}, y^{p-j}, z^{p-j}>$ lies in the octant <+, +, +>. 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)
$x^{p-1} + y^{p-1} - z^{p-1}$

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 multiples 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 $x \le u \le z$, and (B) (1) with continuous, but independent increments in the values of x^{p-1}, y^{p-1} and z^{p-1}.