Revisit of Carmichael 1913 work and an elementary approach for Fermat's Last Theorem of Case I

Gang Li,[1,2,3*]

[1]School of Geophysics and Information Technology
China University of Geosciences (Beijing), Beijing 100083, China
[2]Hansen Experimental Physics Lab, Solar Physics Group
Stanford University, Stanford, CA, USA
[3]Department of Space Science, University of Alabama in Huntsivlle, USA

* send email to: gang.li@uah.edu

May 9, 2018

Abstract

We discuss an elementary approach to prove the first case of Fermat's last theorem (FLT). The essence of the proof is to notice that $a+b+c$ is of order N^α if $a^N+b^N+c^N=0$. To prove FLT, we first show that α can not be 2; we then show that α can not be 3, etc. While this is is the standard method of induction, we refer to it here as the "infinite ascent" technique, in contrast to Fermat's original "infinite descent" technique. A conjecture, first noted by Ribenboim is used.

Introduction

Fermat's Last Theorem asserts that the following equation has no integer solution of a, b, and c when $N \geq 3$.

$$a^N + b^N = c^N. \tag{1}$$

It is one of the most famous mathematical theorem, perhaps due to what Mr. Fermat wrote on the margin of his copy of *Arithmetica of Diophantus*: "I have discovered a truly remarkable

proof of this theorem which this margin is too small to contain."

FLT was proved by Wiles (*1*) and Taylor and Wiles (*2*) in 1994 through proving a special case of the Shimura-Taniyama Conjecture. The proof was by *no* means "elementary", and one wonders if an elementary proof exists.

Some earlier attempts to prove Fermat's last theorem (case I), were to examine the property of the N-th powers modulo N of the triad 1, k, $k+1$. In particular Carmichael (*3,4*) in 1913 showed that if $x^N + y^N + z^N = 0$ has a solution in integers x, y, z each of which is prime to N, then there exists a positive integer s, less than $(p-1)/2$, such that $(1+s)^N - s^N - 1 = 0 \bmod \mathrm{N}^3$.

Extending the earlier work by Carmichael, here we present an elementary approach, called the "**infinite ascending**" to prove case I of FLT. The proof can be applied to arbitrarily many prime numbers. To apply it to all prime numbers, however, the following statement (**hereafter called the RL Conjecture**) needs to be true. This conjecture was first noted by by Ribenboim (see page 61 of *(5)*).

The RL Conjecture: If s is an integer, $1 < s \leq N-2$ where N is a prime number, and if $(1+s)^N - s^N - 1 = 0 \bmod \mathrm{N}^3$, then $s^2 + s + 1 = 0 \bmod \mathrm{N}^3$.

We focus on Case I of FLT here. We discuss case II of FLT in a separate paper.

The Proof

Rewrite equation (1) as,

$$a^N + b^N + c^N = 0. \tag{2}$$

We refer to equation (2) as the FLT below. We make use of the Barlow-Abel relations. These relations are (see e.g. *(5)*).

Barlow-Abel Relation case I: If pairwise relatively prime integers a, b, c satisfy FLT for $N > 2$, and are not multiples of N, then we have

$$a + b = t^N, \frac{a^N + b^N}{a + b} = t_1^N, c = -tt_1 \tag{3}$$

where t and t_1 are co-prime and t_1 is odd. Similar relations exist for $b + c$ and $c + a$.

Consider Case I, from Fermat's little theorem we have,

$$a + b + c = xN^\alpha = (x_0 + \tilde{x}_1 N)N^\alpha, \tag{4}$$

where $\alpha \geq 1$ and $|x_0| < N$. So $a + b + c$ is of order N^α. To prove FLT, below we first show that α can not be 2, then show that α can not be 3, etc. This is the standard method of induction. **However, we will refer to it here as the "infinite ascent" technique in contrast to Fermat's original "infinite descent" technique.**

In the following, we first reproduce a result obtained by Carmichael in 1913. We use a different approach from Carmichael. This is necessary since some of the relationships obtained along the way are needed for the proof .

By multiplying $q < N$, we can always transform a, b, c to the following,

$$a \to 1 + \tilde{a}_1 N, \quad b \to k + \tilde{b}_1 N, \quad c \to -(k + 1) + \tilde{c}_1 N \tag{5}$$

where $1 \leq k \leq N - 2$. Requiring $a^N + b^N + c^N = 0$ leads to the condition

$$1^N + k^N - (k + 1)^N = 0 \mod \mathrm{N}^2 \tag{6}$$

Equation (6) is a constraint on N. For prime numbers smaller than 30, no such k exists for $N = 3, 5, 11, 17, 23, 29$. Therefore case I of FLT is immediately proved for these prime numbers. Now consider prime numbers for which equation (6) is satisfied. For example, $N = 7$, $N = 13$ and $N = 19$. Consider the auxiliary quantity $\Omega = a^N + (b + c)^N$. We have

$$\Omega = (b + c)^N + a^N = (xN^\alpha - a)^N + a^N = x_0 N^{\alpha+1} + O(N^{\alpha+2}). \tag{7}$$

So Ω is of order $N^{\alpha+1}$. From the Barlow-Abel relation, we can write $(b+c)$ as r^N. Therefore,

$$\Omega = (r)^{N^2} + a^N = (r_0 + \tilde{r}_1 N)^{N^2} + (a_0 + \tilde{a}_1 N)^N \tag{8}$$

Clearly, $r^{N^2} = r_0 \pmod{\mathrm{N}}$, so $r_0 = -a_0$. Let $a_0^{N-1} = 1 + m_a N$, we then have,

$$\begin{aligned}
\Omega &= (-a_0 + \tilde{r}_1 N)^{N^2} + (a_0 + \tilde{a}_1 N)^N = -a_0^{N^2} + a_0^{N^2-1}\tilde{r}_1 N^3 + a_0^N + a_0^{N-1}\tilde{a}_1 N^2 + ... \\
&= -a_0^N (1 + m_a N)^N + \tilde{r}_1 N^3 + a_0^N + \tilde{a}_1 N^2 + ... \\
&= (\tilde{a}_1 - m_a a_0) N^2 + O(N^3)
\end{aligned} \tag{9}$$

We now show that α can not be 1. For if so, then the fact that $a+b+c$ is of order N^α yields $a_1 + b_1 + c_1 = x_0$. From equation (7) and (9) we have to have,

$$(a_1 - m_a a_0) = x_0 \bmod \mathrm{N} \tag{10}$$

Similarly, by considering $(a+b)^N + c^N$ and $(c+a)^N + b^N$, we obtain,

$$(b_1 - m_b b_0) = x_0 \bmod \mathrm{N}, \quad (c_1 - m_c c_0) = x_0 \bmod \mathrm{N} \tag{11}$$

where $b_0^{N-1} = 1 + m_b N$ and $c_0^{N-1} = 1 + m_c N$ are understood.

Adding equations (10) and (11) together we see that,

$$m_a a_0 + m_b b_0 + m_c c_0 + 2x_0 = 0 \ \bmod \mathrm{N} \tag{12}$$

On the other hand we have,

$$\begin{aligned}
a^N + b^N + c^N &= a_0^N + b_0^N + c_0^N + (a_1 + b_1 + c_1) N^2 + O(N^3) \\
&= a_0(1 + m_a N) + b_0(1 + m_b N) + c_0(1 + m_c N) + x_0 N^2 + O(N^3) \\
&= (a_0 m_a + b_0 m_b + c_0 m_c) N + x_0 N^2 + O(N^3).
\end{aligned} \tag{13}$$

where we have used $a_0 + b_0 + c_0 = 0$. So

$$a_0 m_a + b_0 m_b + c_0 m_c = -x_0 N \ \bmod \mathrm{N}^2. \tag{14}$$

Therefore

$$a_0 m_a + b_0 m_b + c_0 m_c = 0 \mod \mathrm{N} \tag{15}$$

So equation (12) contradicts with (15). Therefore we must have $x_0 = 0$ and $\alpha \geq 2$.

If $x_0 = 0$ and $\alpha \geq 2$, we can expand a, b and c to,

$$a = a_0 + a_1 N + \tilde{a}_2 N^2, \quad b = b_0 + b_1 N + \tilde{b}_2 N^2, \quad c = c_0 + c_1 N + \tilde{c}_2 N^2 \tag{16}$$

with $a_0 + b_0 + c_0 = 0$ and $a_1 + b_1 + c_1 = 0$. Equations (10) and (11) become,

$$a_1 = m_a a_0 \bmod \mathrm{N}, \quad b_1 = m_b b_0 \bmod \mathrm{N}, \quad c_1 = m_c c_0 \bmod \mathrm{N}, \tag{17}$$

So,

$$a = a_0(1 + m_a N) + ..., \quad b = b_0(1 + m_b N) + ..., \quad c = c_0(1 + m_c N) + ..., \tag{18}$$

Or,

$$a = a_0^N + \tilde{a}_2' N^2, \quad b = b_0^N + \tilde{b}_2' N^2, \quad c = c_0^N + \tilde{c}_2' N^2 \tag{19}$$

Since $a_1 + b_1 + c_1 = 0$, from the first line of equation (13) we have,

$$a_0^N + b_0^N + c_0^N = 0 \bmod \mathrm{N}^3 \tag{20}$$

Note that if $a+b+c$ is of order N^2, then $\tilde{a}_2'$, $\tilde{b}_2'$ and $\tilde{c}_2'$ in equation (19) has to satisfy, $\tilde{a}_2' + \tilde{b}_2' + \tilde{c}_2' = \Delta' N^2$ where $\Delta' \neq 0 \bmod \mathrm{N}$. Let $q = a_0^{-1}$, i.e., $a_0 q = 1 + \epsilon_a N$. Denote $b_0 q = k + \epsilon_b N$, and $c_0 q = -(k+1) + \epsilon_c N$. Multiply q^N to equation (19), let $a_{new} = q^N a$, $b_{new} = q^N b$, and $c_{new} = q^N c$, we find,

$$a_{new} = (a_0 q)^N + (\tilde{a}_2' q^N) N^2 = (1 + \epsilon_a N)^N + (\tilde{a}_2' q^N) N^2 = 1 + \tilde{a}_2'' N^2 \tag{21}$$

$$b_{new} = (b_0 q)^N + (\tilde{b}_2' q^N) N^2 = (k + \epsilon_b N)^N + (\tilde{b}_2' q^N) N^2 = k^N + \tilde{b}_2'' N^2 \tag{22}$$

$$c_{new} = (c_0 q)^N + (\tilde{c}_2' q^N) N^2 = (-(k+1) + \epsilon_c N)^N + (\tilde{c}_2' q^N) N^2 = -(k+1)^N + \tilde{c}_2'' N^2 \tag{23}$$

Define m and m' through,

$$k^{N-1} = 1 + mN, \quad (k+1)^{N-1} = 1 + m'N, \tag{24}$$

Equations (22) and (23) can be rewritten as,

$$b_{new} = k + kmN + \tilde{b}_2'''N^2 \tag{25}$$

$$c_{new} = -(k+1) - (k+1)m'N + \tilde{c}_2'''N^2 \tag{26}$$

Since $(a+b+c)$ is of order N^α, so $a_{new} + b_{new} + c_{new}$ is also of order N^α. Because $\alpha \geq 2$, we must have,

$$km = (k+1)m' \bmod \mathrm{N}. \tag{27}$$

So we can write,

$$km = b_1 + \tilde{b}_2 N, \text{ and } (k+1)m' = b_1 + \tilde{c}_2 N, \tag{28}$$

where we have reused the symbols $\tilde{b}_2$ and $\tilde{c}_2$. Requiring $a_{new}^N + b_{new}^N + c_{new}^N = 0$ leads to,

$$1 + k^N - (k+1)^N = 0 \bmod \mathrm{N}^3, \text{ or } 1 + k^N - (k+1)^N = \delta N^3, \tag{29}$$

This relationship was obtained by Carmichael in 1913. This is a stronger constraint than equation (6). Of the 167 (1228) prime numbers smaller than 1000 (10000), 80 (611) of them, i.e. only 50% of them have k's satisfy equation (29). We further assume δ in equation (29) satisfy $\delta \neq 0 \bmod \mathrm{N}$ (see (35) and (36) for justification).

Since $1 + k^N - (k+1)^N = 1 + k(1+mN) - (k+1)(1+m'N)$, with the condition (29), equation (27) becomes,

$$km = (k+1)m' \bmod \mathrm{N}^2, \tag{30}$$

If the set $[1, k, -(k+1)]$ satisfies the requirement (29), then the set $[1, k-N, N-(k+1)]$ also satisfies (29). Denote this as the adjoint set. We will regard these two as the same set. Denote $q < N$ to be k^{-1}, i.e., $qk = 1 \pmod{\mathrm{N}}$, then we can generate another set $[q, 1, -(q+1)]$ which

also satisfies (29). Denote $k^* = N - (q+1)$, with its inverse to be q^*, then the adjoint set of $[q, 1, -(q+1)]$ is $[q-N, 1, N-(q+1)] = [-(k^*+1), 1, k^*]$; from which we can multiply q^* to generate another set $[-(q^*+1), q^*, 1]$. So from one set $[1, k, -(k+1)]$ we obtain three sets $[1, k, -(k+1)]$, $[q, 1, -(q+1)]$ and $[-(q^*+1), q^*, 1]$. These three sets are either distinct or they can be the *same*. **They are the same if the RL conjecture is true. And vice versa.** A quick check of all prime numbers smaller than 10000 shows that if the requirement (29) is satisfied, then only one set of $[1, k, k+1]$ exists, i.e., the three sets $[1, k, -(k+1)]$, $[q, 1, -(q+1)]$ and $[-(q^*+1), q^*, 1]$ are the same.

Definition: a prime number N is called a k^3-prime if the condition (29) is satisfied by one and only one set of $[1, k, -(k+1)]$ (not counting adjoint sets). In the following we prove case I of FLT for k^3-primes.

For any given prime number p, it is straightforward to verify if p is a k^3-prime by examining the condition (29).

If N is a k^3-prime, then the three sets which are generated from the single set $[1, k, -(k+1)]$ are the same, so we must have,

$$-(k+1) = k^2 - \beta N \text{ where } 1 < \beta < N-1. \tag{31}$$

From equation (31), we also obtain $k^2+k+1 = \beta N$, $k(k+1) = -1+\beta N$, $k^3 = 1+(k-1)\beta N$, and $k(k+2) = (k-1) + \beta N$. Furthermore, from equation (30) we have,

$$m' = (k+1)m \bmod \mathrm{N}. \tag{32}$$

We can multiply k^N and k^{2N} to the requirement (29) to obtain,

$$k^N + k^{2N} - (k(k+1))^N = \delta k^N N^3, \tag{33}$$

$$k^{2N} + k^{3N} - (k^2(k+1))^N = \delta k^{2N} N^3, \tag{34}$$

Using equation (24), the requirements (29), (33) and (34) yield the following relationships:

$$\beta = (k+2)m \mod \mathrm{N}, \tag{35}$$

$$(k+1)m^2 + 2\delta = 0 \mod \mathrm{N}. \tag{36}$$

From equation (35) and (36), we see that $\delta \neq 0$ modN. For if so, $m = 0$ and $\beta = 0$, but from equation (31), it is clear $\beta \neq 0$ for k^3-primes. Using $k(k+1) = -1$modN, equation (36) can be also written as,

$$m^2k^2 = 2\delta \mod \mathrm{N}. \tag{37}$$

ascending α from 2 to 3

Assuming $\alpha = 2$, i.e. $a + b + c$ is of order N^2. Let us suppose a_{new}, b_{new} and c_{new} in equations (21), (22), and (23) satisfy $a_{new} + b_{new} + c_{new} = \Delta_2 N^2 + O(N^3)$ where Δ_2 is to remind us that we are on level II of the "infinite ascending ladder". By multiplying terms in the form of $1 - w_l N^l$ to a_{new}, b_{new} and c_{new} with $l = 2$ (this operation leaves Δ_2 unchanged), we can transform a_{new}, b_{new}, and c_{new} into,

$$a_{new} \to a = 1 + \Delta_2 N^2 + \tilde{a}_3 N^3 \tag{38}$$

$$b_{new} \to b = k^N + b_2 N^2 + \tilde{b}_3 N^3 = k + b_1 N + b'_2 N^2 + \tilde{b}'_3 N^3 \tag{39}$$

$$c_{new} \to c = -(k+1)^N - b_2 N^2 + \tilde{c}_3 N^3 = -(k+1) - b_1 N - b'_2 N^2 + \tilde{c}'_3 N^3 \tag{40}$$

where b_1 satisfies $km = b_1 \pmod{\mathrm{N}}$, as can be seen from equation (28). For convenience we re-use a, b, c in these equations. To the order of N^3, using $k(k+1) = -1 \bmod \mathrm{N}$, we have

$$k(k+1)(a^N + b^N + c^N) = \{-(\delta + \Delta_2) + kmb_1 + \frac{N-1}{2} b_1^2\} N^3 + O(N^4) \tag{41}$$

In equations (41) the coefficient of N^3 must equal to zero. So,

$$(b_1 - km)^2 = -2\Delta_2 \mod \mathrm{N} \tag{42}$$

Since $b_1 = km \pmod{\mathrm{N}}$, so Δ_2 is zero. Therefore we have $\alpha \geq 3$.

ascending α from 3 to infinity

We next suppose $a_{new} + b_{new} + c_{new} = \Delta_3 N^3 + O(N^4)$. Following the same procedure as in equations (38), (39) and (40), i.e., multiplying terms in the form of $1 - w_l N^l$ to a_{new}, b_{new} and c_{new} with $l \geq 2$, we find, to order N^4,

$$a_{new} \to a = 1 + (\Delta_3 - \delta)N^3 + \tilde{a}_4 N^4 \quad (43)$$

$$b_{new} \to b = k^N + (b_2 N^2 + b_3 N^3) + \tilde{b}_4 N^4 \quad (44)$$

$$c_{new} \to c = -(k+1)^N - (b_2 N^2 + b_3 N^3) + \tilde{c}_4 N^4 \quad (45)$$

Again we still have $a + b + c = \Delta_3 N^3 + O(N^4)$ since the transformation from $a_{new} \to a$, $b_{new} \to b$, and $c_{new} \to c$ do not change Δ_3.

Using equations (43), (44) and (45), to order N^4 we have,

$$\begin{aligned} & a^N + b^N + c^N = 1 + k^{N^2} - (k+1)^{N^2} = 1 + k^N(1+mN)^N - (k+1)^N(1+m'N)^N \\ & = 1 + k^N(1 + mN^2 + \frac{N-1}{2}m^2N^3) - (k+1)^N(1 + m'N^2 + \frac{N-1}{2}(m')^2N^3) \\ & = \delta N^3 + mkN^2(k^{N-1} - (k+1)^{N-1}) + \frac{N-1}{2}mkN^3(mk^{N-1} - m'(k+1)^{N-1}) \\ & = N^3\{\delta + \frac{1}{2}mk(m-m')\} \end{aligned} \quad (46)$$

where we have used $km = m'(k+1) \bmod \mathrm{N}$. Using equation (29) for δ, equation (32) for m', and multiply by $2k^3$, equation (46) becomes,

$$2k^3(a^N + b^N + c^N) = k^2N^3(m^2 - m^2k^3) = 0 \bmod \mathrm{N}^4 \quad (47)$$

So indeed $a^N + b^N + c^N = 0$ up to order N^3. Next to order N^4, using equations (43), (44) and (45) again, we have,

$$a^N + b^N + c^N = 1 + k^{N^2} - (k+1)^{N^2} + (\Delta_3 - \delta)N^4 \quad (48)$$

Now that from equation (46) we know $1 + k^{N^2} - (k+1)^{N^2}$ is zero up to order N^3, so we can let $1 + k^{N^2} - (k+1)^{N^2} = \epsilon N^4$. Multiply by k^{N^2}, we obtain,

$$k^{N^2}(1 + k^{N^2} - (k+1)^{N^2}) = k^{N^2}\epsilon N^4. \tag{49}$$

To order N^4, the RHS of equation (49) is $k\epsilon N^4$. The LHS is,

$$\begin{aligned} LHS &= k^{N^2} + (k^2)^{N^2} - (k(k+1))^{N^2} = k^{N^2} + (\beta N - (k+1))^{N^2} + (1-\beta N)^{N^2} \\ &= 1 + k^{N^2} - (k+1)^{N^2} + ((k+1)^{N^2-1} - 1)\beta N^3 \\ &\quad + \frac{1}{2}N^4(N^2-1)\beta^2(1 - (k+1)^{N^2-2}) \\ &= \epsilon N^4 + \beta m' N^4 - \frac{\beta^2 N^4}{2(k+1)}(k+1-1) = N^4(\epsilon + \beta m' - \frac{\beta^2 k^2}{2k(k+1)}) \end{aligned} \tag{50}$$

Equating LHS and RHS,

$$2k(k+1)(k-1)\epsilon = 2k(k+1)\beta m' - \beta^2 k^2, \quad \text{mod N} \tag{51}$$

Using $k(k+1) = -1 \pmod{\text{N}}$, $k - 1 = k(k+2) \pmod{\text{N}}$, $\beta = (k+2)m \pmod{\text{N}}$, and $m' = (k+1)m \pmod{\text{N}}$, we find,

$$2k\epsilon = 2(k+1)m^2 + (k+2)m^2k^2 \;\; \rightarrow 2\epsilon = k^2m^2 = 2\delta \quad \text{mod N} \tag{52}$$

Since $\epsilon = \delta \bmod \text{N}$, therefore from equation (48) we see that Δ_3 must be zero. Now we can apply this recursively ("infinitely ascend") to obtain $\Delta_\gamma = 0$ and $(1 + k^{N^{\gamma-1}} - (k+1)^{N^{\gamma-1}}) = \delta N^{\gamma+1} + O(N^{\gamma+2})$.

Now assuming $\Delta_\gamma = 0$ and $(1 + k^{N^{\gamma-1}} - (k+1)^{N^{\gamma-1}}) = \delta N^{\gamma+1} + O(N^{\gamma+2})$, we show that $\Delta_{\gamma+1} = 0$ and $(1 + k^{N^\gamma} - (k+1)^{N^\gamma}) = \delta N^{\gamma+2} + O(N^{\gamma+3})$.

We make use of $(k+1)^{N^\gamma - 1} = (k+1)^{(N-1)(1+N+N^2+...+N^{\gamma-1})} = (1+m'N)(1+m'N)^N(1+m'N)^{N^2}...(1+m'N)^{N^{\gamma-1}} = 1 + m'N + ...$, and similar expression for $k^{N^\gamma - 1}$ ($k^{N^\gamma-1} = 1 + mN + ...$).

First, equations (43), (44) and (45) are now,

$$a_{new} \to a = 1 + (\Delta_{\gamma+1} - \delta)N^{\gamma+1} + \tilde{a}_{\gamma+2}N^{\gamma+2} \quad (53)$$

$$b_{new} \to b = k^{N^{\gamma-1}} + (b_2N^2 + ... + b_{\gamma+1}N^{\gamma+1}) + \tilde{b}_{\gamma+2}N^{\gamma+2} \quad (54)$$

$$c_{new} \to c = -(k+1)^{N^{\gamma-1}} - (b_2N^2 + ... + b_{\gamma+1}N^{\gamma+1}) + \tilde{c}_{\gamma+2}N^{\gamma+2} \quad (55)$$

For example, if $\gamma = 3$, we have

$$a_{new} \to a = 1 + (\Delta_4 - \delta)N^4 + \tilde{a}_5N^5 \quad (56)$$

$$b_{new} \to b = k^{N^2} + (b_2N^2 + b_3N^3 + b_4N^4) + \tilde{b}_5N^5 \quad (57)$$

$$c_{new} \to c = -(k+1)^{N^2} - (b_2N^2 + b_3N^3 + b_4N^4) + \tilde{c}_5N^5 \quad (58)$$

If $(1 + k^{N^{\gamma-1}} - (k+1)^{N^{\gamma-1}}) = \delta N^{\gamma+1} + O(N^{\gamma+2})$, then up to order $N^{\gamma+1}$, we find,

$$\begin{aligned}
& 1 + k^{N^\gamma} - (k+1)^{N^\gamma} = 1 + k^{N^{\gamma-1}}k^{(N-1)N^{\gamma-1}} - (k+1)^{N^{\gamma-1}}(k+1)^{(N-1)N^\gamma} \\
= \; & 1 + k^{N^{\gamma-1}}(1+mN)^{N^{\gamma-1}} - (k+1)^{N^{\gamma-1}}(1+m'N)^{N^\gamma} \\
= \; & (1 + k^{N^{\gamma-1}} - (k+1)^{N^{\gamma-1}}) + (mk^{N^{\gamma-1}} - m'(k+1)^{N^{\gamma-1}})N^\gamma \\
& + \frac{N^{\gamma+1}(N^{\gamma-1}-1)}{2}(m^2k^{N^{\gamma-1}} - m'^2(k+1)^{N^{\gamma-1}}) + ... \\
= \; & \delta N^{\gamma+1} + (mk^{N^{\gamma-1}} - m'(1 + k^{N^{\gamma-1}} - \delta N^{\gamma+1}))N^\gamma - \frac{N^{\gamma+1}}{2}(m^2k - m'^2(k+1)) + ... \\
= \; & \delta N^{\gamma+1} + ((m-m')k^{N^{\gamma-1}} - m')N^\gamma + \frac{N^{\gamma+1}}{2}(m'^2(k+1) - m^2k) + ... \\
= \; & \delta N^{\gamma+1} + ((m-m')k(1+mN) - m')N^\gamma + \frac{N^{\gamma+1}}{2}(m'-m)mk + ... \\
= \; & \delta N^{\gamma+1} + ((mk - m'(k+1)) - k^2m^2N)N^\gamma + \frac{N^{\gamma+1}}{2}m^2k^2 + ... \\
= \; & (\delta - \frac{1}{2}k^2m^2)N^{\gamma+1} + ... = 0
\end{aligned} \quad (59)$$

where in the last step we used equation (37). So we can let $(1 + k^{N^\gamma} - (k+1)^{N^\gamma}) = \epsilon N^{\gamma+2} + O(N^{\gamma+3})$. Multiply by k^{N^γ}, we obtain,

$$k^{N^\gamma}(1 + k^{N^\gamma} - (k+1)^{N^\gamma}) = k^{N^\gamma}\epsilon N^{\gamma+2}. \quad (60)$$

To the order $N^{\gamma+2}$, the RHS of equation (49) is $k\epsilon N^{\gamma+2}$. The LHS is,

$$\begin{aligned} LHS &= k^{N^\gamma} + (k^2)^{N^\gamma} - (k(k+1))^{N^\gamma} = k^{N^\gamma} + (\beta N - (k+1))^{N^\gamma} + (1-\beta N)^{N^\gamma} \\ &= 1 + k^{N^\gamma} - (k+1)^{N^\gamma} + ((k+1)^{N^\gamma - 1} - 1)\beta N^{\gamma+1} \\ &\quad + \frac{1}{2} N^\gamma (N^\gamma - 1)\beta^2 N^2 (1 - (k+1)^{N^\gamma - 2}) \\ &= \epsilon N^{\gamma+2} + \beta m' N^{\gamma+2} - \frac{\beta^2 N^{\gamma+2}}{2(k+1)} (k + 1 - (k+1)^{N^\gamma - 1}) \\ &= N^{\gamma+2} (\epsilon + \beta m' - \frac{\beta^2 k^2}{2k(k+1)}) \end{aligned} \tag{61}$$

Equating LHS and RHS, we find the same equation (52) and $\epsilon = \delta$. So, $\Delta_{\gamma+1}$ must be zero. We can continue this procedure and find $a + b + c = 0 \pmod{\mathrm{N}^\tau}$, with τ arbitrarily large. This is absurd. Therefore Case I of FLT (for k^3-primes) is proved.

Discussion

Mr. Fermat is arguably the best amateur mathematician in history. Less known is that he was also a very insightful physicist. He discovered that between two points light travels along a path which yields the least travel time. This stimulated the later development of the least action principle in theoretical physics. Perhaps Mr. Fermat's impact to Physics is no less than his contribution to Mathematics.

Could the approach presented here the one Mr. Fermat was thinking when he made his famous remark in the margin of his copy of *Arithmetica of Diophantus*? Possibly, but we may never know. It could well be that Mr. Fermat had an even better proof.

Acknowledgment: This work was started when I took a full-year sabbatical leave from the Department of Space Science at the University of Alabama in Huntsville. During this span, I took a guest professor position at the School of Geophysics and Information Technology, China University of Geosciences (Beijing), Beijing, China; and a visiting scholar position at

the Hansen Experimental Physics Lab at the Stanford University, CA, USA. I thank Dr. Shuo Yao for her help during my stay in Beijing and Dr. Xudong Sun for his help during my stay in Stanford. I also thank Dr. Yao Chen and Dr. Yong Jiang for their hospitality during my visits to ShanDong University at Weihai and Nanjing University of Information and Science Technology. Last but not least, I must thank my brother, Qiang Li, without whom this work can never be completed.

References and Notes

1. Wiles, A., *Ann. Math.* **141**, 443-551, (1995).

2. Taylor, R. and Wiles, A., *Ann. Math.* **141**, 553-572, (1995).

3. Carmichael, R. D., Bull. Amer. Math. Soc., 19, 233-236, (1913).

4. Carmichael, R. D., Bull. Amer. Math. Soc., 19, 1913, 402-403, (1913).

5. Ribenboim, Paulo, *13 lectures on Fermat's last theorem*, Verlag: Springer. (1979).