On Fermat's Last Theorem – An Elementary Approach

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

[*] On sabbatical leave from UAHuntsville, send email to: gang.li@uah.edu

June 14, 2017

An attempt of using elementary approach to prove Fermat's last theorem (FLT) is given. For infinitely many prime numbers, Case I of the FLT can be proved using this approach. Furthermore, if a conjecture proposed in this paper is true (k^3-conjecture), then case I of the FLT is proved for all prime numbers. For case II of the FLT, a constraint for possible solutions is obtained.

Introduction

Fermat's Last Theorem (conjecture before 1995) asserts that the following equation has no integer soluation 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." Ever since then many generations of mathematician have attempted to find such a proof. Some 350 years later, the conjecture 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.

Here we present an approach to prove case I of FLT.

The Proof

We prove it by the method of contradiction. We only need to prove it for N being an odd prime number. Rewrite equation (1) to,

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

We refer to equation (2) as the FLT below. As done previously by many workers, we separate the proof to two cases (case I and II) according to if N divides one of a, b, c. We make use of the Barlow-Abel relations. These relations are (e.g. *3*).

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 $c + a$.

Barlow-Abel Relation case II: If $N \mid c$ and $N \nmid (ab)$, then we have,

$$\begin{aligned} a + b &= N^{\alpha N - 1} t^N, \frac{a^N + b^N}{a + b} = N t_1^N, c = -N^\alpha t t_1, && (4) \\ b + c &= r^N, \frac{b^N + c^N}{b + c} = r_1^N, a = -r r_1 && (5) \\ c + a &= s^N, \frac{c^N + a^N}{c + a} = s_1^N, b = -s s_1 && (6) \end{aligned}$$

where t and t_1 are co-prime and t_1 is odd; r and r_1 are co-prime and r_1 is odd; s and s_1 are co-prime and s_1 is odd.

A notation: Any number a can be written as $a = a_0 + \tilde{a}_1 N$, where $0 \leq |a_0| \leq N - 1$. And $\tilde{a}_1$ can be further written as $\tilde{a}_1 = a_1 + \tilde{a}_2 N$. Clearly, $\tilde{a}_i = a_i \pmod{\mathrm{N}}$. In the following, we use this notation for a, b and c, but not other variables.

Case I: $N \nmid (abc)$, i.e. N is relatively prime to a, b and c. From Fermat's little theorem we have,

$$a + b + c = xN^\alpha = (x_0 + \tilde{x}_1 N)N^\alpha, \tag{7}$$

where $\alpha \geq 1$ and $|x_0| < N$. So $a + b + c$ is of order N^α.

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

$$\begin{aligned} a &\rightarrow 1 + \tilde{a}_1 N & (8)\\ b &\rightarrow k + \tilde{b}_1 N & (9)\\ c &\rightarrow -(k+1) + \tilde{c}_1 N & (10) \end{aligned}$$

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

$$1^N + k^N - (k+1)^N = 0 \mod \mathrm{N}^2 \tag{11}$$

Equation (11) is a rather strong constraint on N. For prime numbers smaller than 30, no such k exists for $N = 3$, 5, 11, 17, 23, 29. Therefore Fermat's Last Theorem for case I is immediatedly proved for these prime numbers. We now consider prime numbers for which equation (11) is satisfied. For example, $N = 7$, $N = 13$ and $N = 19$. Consider the auxiliary quantity $\Omega = a^N + (b+c)^N$. We have

$$\Omega = (b+c)^N + a^N = (xN^\alpha - a)^N + a^N = x_0 N^{\alpha+1} + O(N^{\alpha+2}). \tag{12}$$

So Ω is of order $N^{\alpha+1}$.

From the Barlow-Abel relation, we can write $(b+c)$ as r^N. Therefore,

$$\Omega = (r)^{N^2} + a^N = (r_0 + \tilde{r}_1 N)^{N^2} + (a_0 + \tilde{a}_1 N)^N \tag{13}$$

Clearly, $r^{N^2} = r_0$ (mod N), so $r_0 = -a_0$. Let $a_0^{N-1} = 1 + m_a N$, we then have,

$$\begin{aligned}\Omega &= (-a_0 + \tilde{r}_1 N)^{N^2} + (a_0 + \tilde{a}_1 N)^N = -a_0^{N^2} + a_0^{N^2-1}\tilde{r}_1 N^3 + a_0^N + a_0^{N-1}\tilde{a}_1 N^2 + ... \\ &= -a_0^N (1 + m_a N)^N + \tilde{r}_1 N^3 + a_0^N + \tilde{a}_1 N^2 + ... \\ &= (\tilde{a}_1 - m_a a_0) N^2 + O(N^3) \end{aligned} \tag{14}$$

We first 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 (12) and (14) we have to have,

$$(a_1 - m_a a_0) = x_0 \text{ mod N} \tag{15}$$

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

$$(b_1 - m_b b_0) = x_0 \text{ mod N}, \quad (c_1 - m_c c_0) = x_0 \text{ mod N} \tag{16}$$

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

Adding equations (15) and (16) together we see that,

$$m_a a_0 + m_b b_0 + m_c c_0 + 2x_0 = 0 \ \text{ mod N} \tag{17}$$

On the other hand we have,

$$\begin{aligned} a^N + b^N + c^N &= a_0^N + b_0^N + c_0^N + (a_1 + b_1 + c_1) N^2 + O(N^3) \\ &= a_0(1 + m_a N) + b_0(1 + m_b N) + c_0(1 + m_c N) + x_0 N^2 + O(N^3) \\ &= (a_0 m_a + b_0 m_b + c_0 m_c) N + x_0 N^2 + O(N^3). \end{aligned} \tag{18}$$

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

$$a_0 m_a + b_0 m_b + c_0 m_c = -x_0 N \ \text{ mod N}^2. \tag{19}$$

Therefore

$$a_0 m_a + b_0 m_b + c_0 m_c = 0 \mod \mathrm{N} \tag{20}$$

So equation (17) contradicts with (20). 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,

$$a = a_0 + a_1 N + \tilde{a}_2 N^2, \quad b = b_0 + b_1 N + \tilde{b}_2 N^2, \quad c = c_0 + c_1 N + \tilde{c}_2 N^2 \tag{21}$$

with $a_0 + b_0 + c_0 = 0$ and $a_1 + b_1 + c_1 = 0$. Equations (15) and (16) become,

$$a_1 = m_a a_0 \bmod \mathrm{N}, \quad b_1 = m_b b_0 \bmod \mathrm{N}, \quad c_1 = m_c c_0 \bmod \mathrm{N}, \tag{22}$$

So,

$$a = a_0(1 + m_a N) + ..., \quad b = b_0(1 + m_b N) + ..., \quad c = c_0(1 + m_c N) + ..., \tag{23}$$

Or,

$$a = a_0^N + \tilde{a}'_2 N^2, \quad b = b_0^N + \tilde{b}'_2 N^2, \quad c = c_0^N + \tilde{c}'_2 N^2 \tag{24}$$

Since $a_1 + b_1 + c_1 = 0$, from the first line of equation (18) we have,

$$a_0^N + b_0^N + c_0^N = 0 \bmod \mathrm{N}^3 \tag{25}$$

Note that if $a+b+c$ is of order N^2, then $\tilde{a}'_2$, $\tilde{b}'_2$ and $\tilde{c}'_2$ in equation (24) 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 (24), let $a_{new} = q^N a$, $b_{new} = q^N b$, and $c_{new} = q^N c$, we find,

$$a_{new} = (a_0 q)^N + (\tilde{a}'_2 q^N) N^2 = (1 + \epsilon_a N)^N + (\tilde{a}'_2 q^N) N^2 = 1 + \tilde{a}''_2 N^2 \tag{26}$$

$$b_{new} = (b_0 q)^N + (\tilde{b}'_2 q^N) N^2 = (k + \epsilon_b N)^N + (\tilde{b}'_2 q^N) N^2 = k^N + \tilde{b}''_2 N^2 \tag{27}$$

$$c_{new} = (c_0 q)^N + (\tilde{c}'_2 q^N) N^2 = (-(k+1) + \epsilon_c N)^N + (\tilde{c}'_2 q^N) N^2 = -(k+1)^N + \tilde{c}''_2 N^2 \tag{28}$$

Define m and m' through,

$$k^{N-1} = 1 + mN, \quad (k+1)^{N-1} = 1 + m'N, \tag{29}$$

Equations (27) and (28) can be rewritten as,

$$b_{new} \;=\; k + kmN + \tilde{b}_2'''N^2 \tag{30}$$

$$c_{new} \;=\; -(k+1) - (k+1)m'N + \tilde{c}_2'''N^2 \tag{31}$$

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 have

$$km = (k+1)m' \text{ mod N} \tag{32}$$

So, we can write

$$km = b_1 + \tilde{b}_2 N, \text{ and } (k+1)m' = b_1 + \tilde{c}_2 N, \tag{33}$$

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,

$$1 + k^N - (k+1)^N = 0 \text{ mod N}^3, \text{ or } 1 + k^N - (k+1)^N = \delta N^3, \; \delta \neq 0 \text{ mod N} \tag{34}$$

This is an even stronger condition than equation (11). 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 (34). With the condition (34), equation (32) becomes,

$$km = (k+1)m' \text{ mod N}^2, \tag{35}$$

If the set $[1, k, -(k+1)]$ satisfies the requirement (34), then the set $[1, k-N, N-(k+1)]$ also satisfies (34). Denote this as the adjoint set. We will regard these two as the same set. Denote $q < N$ to be k^{-1}, i.e., $qk = 1$ (mod N), then we can generate another set $[q, 1, -(q+1)]$ which also satisfies (34). 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**.

A quick check of all prime numbers smaller than 10000 shows that if the requirement (34) 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 (34) is satisfied by one and only one set of $[1, k, -(k+1)]$ (not counting adjoint sets). For k^3-primes, case I of FLT can be proved in below. **The k^3 conjecture: All prime numbers which satisfy condition (34) are k^3-primes.** For any given prime number N, it is straightforward to verify the condition (34), therefore if the k^3 conjecture is true. However, the author failed to see a simple argument to prove he k^3-conjecture.

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,

$$-(k+1) = k^2 - \beta N \text{ where } 1 < \beta < N-1. \tag{36}$$

From equation (36), 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 (35) we have,

$$m' = (k+1)m \bmod \mathrm{N}^2. \tag{37}$$

We can multiply k^N and k^{2N} to the requirement (34) to obtain,

$$\begin{aligned} k^N + k^{2N} - (k(k+1))^N &= \delta k^N N^3, & (38)\\ k^{2N} + k^{3N} - (k^2(k+1))^N &= \delta k^{2N} N^3, & (39)\end{aligned}$$

Using equation (29), the requirements (34), (38) and (39) yield the following relationships:

$$\beta = (k+2)m \mod \mathrm{N} \tag{40}$$

$$(k+1)m^2 + 2\delta = 0 \mod \mathrm{N} \tag{41}$$

where δ in equation (41) is defined in equation (34).

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.**

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

$$\begin{aligned} a_{new} \to a &= 1 + \Delta_2 N^2 + \tilde{a}_3 N^3 & (42)\\ b_{new} \to b &= k^N + b_2 N^2 + \tilde{b}_3 N^3 = k + b_1 N + b_2' N^2 + \tilde{b}_3' N^3 & (43)\\ c_{new} \to c &= -(k+1)^N - b_2 N^2 + \tilde{c}_3 N^3 = -(k+1) - b_1 N - b_2' N^2 + \tilde{c}_3' N^3 & (44) \end{aligned}$$

where b_1 satisfies $km = b_1 \pmod{\mathrm{N}}$, as can be seen from equation (33). For convenience we re-use a, b, c in these equations. To the order of N^3, using $k(k+1) = -1$ (mod N), we have

$$k(k+1)(a^N + b^N + c^N) = \{-(\delta + \Delta_2) + kmb_1 + \frac{N-1}{2} b_1^2\} N^3 + O(N^4) \tag{45}$$

In equations (45) the coefficient of N^3 must equal to zero. So,

$$(b_1 - km)^2 = -2\Delta_2 \mod \mathrm{N} \tag{46}$$

Since $b_1 = km$ (mod N), so Δ_2 is zero. Therefore we have $\alpha \geq 3$.

We next suppose $a_{new} + b_{new} + c_{new} = \Delta_3 N^3 + O(N^4)$. Following the same procedure as in equations (42), (43) and (44), we find, to order N^4,

$$\begin{aligned} a_{new} \to a &= 1 + (\Delta_3 - \delta)N^3 + \tilde{a}_4 N^4 && (47) \\ b_{new} \to b &= k^N + (b_2 N^2 + b_3 N^3) + \tilde{b}_4 N^4 && (48) \\ c_{new} \to c &= -(k+1)^N - (b_2 N^2 + b_3 N^3) + \tilde{c}_4 N^4 && (49) \end{aligned}$$

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. So,

$$\begin{aligned} a + b + c &= 1 + k^N - (k+1)^N + (\Delta_3 - \delta)N^3 + \{(1 + mN) - (1 + m'N)\}b_2 N^2 + O(N^4) \\ &= \Delta_3 N^3 + (m - m')b_2 N^3 + O(N^4) \\ &= (\Delta_3 + (m - m')b_2)N^3 + O(N^4) && (50) \end{aligned}$$

From equations (42), (43), (44), and noticing $\Delta_2 = 0$, we find, to order N^3,

$$\begin{aligned} & a^N + b^N + c^N = 1 + k^{N^2} - (k+1)^{N^2} = 1 + k^N(1 + mN)^N - (k+1)^N(1 + m'N)^N \\ & = 1 + k^N(1 + mN^2 + \frac{N-1}{2}m^2N^3) - (k+1)^N(1 + m'N^2 + \frac{N-1}{2}(m')^2N^3) \\ & = \delta N^3 + mkN^2(k^{N-1} - (k+1)^{N-1}) + \frac{N-1}{2}mkN^3(mk^{N-1} - m'(k+1)^{N-1}) \\ & = N^3\{\delta + \frac{1}{2}mk(m - m')\} && (51) \end{aligned}$$

where we have used $km = m'(k+1) \pmod{\mathrm{N}}$. Using equation (34) for δ, equation (37) for m', and multiply by $2k^3$, equation (51) becomes,

$$2k^3(a^N + b^N + c^N) = k^2N^3(m^2 - m^2k^3) = 0 \bmod \mathrm{N}^4 \qquad (52)$$

So indeed $a^N + b^N + c^N = 0$ up to order N^3. Using equations (47), (48) and (49), we have, to order N^4,

$$a^N + b^N + c^N = 1 + k^{N^2} - (k+1)^{N^2} + (\Delta_3 - \delta)N^4 \qquad (53)$$

Now that from equation (51) 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,

$$k^{N^2}(1 + k^{N^2} - (k+1)^{N^2}) = k^{N^2}\epsilon N^4. \tag{54}$$

To order N^4, the RHS of equation (54) is $k\epsilon N^4$. The LHS is,

$$\begin{aligned} LHS &= k^{N^2} + (k^2)^{N^2} - (k(k+1))^{N^2} = k^{N^2} + (\beta N - (k+1))^{N^2} + (1 - \beta N)^{N^2} \\ &= 1 + k^{N^2} - (k+1)^{N^2} + ((k+1)^{N^2-1} - 1)\beta N^3 \\ &\quad + \frac{1}{2}N^4(N^2-1)\beta^2(1 - (k+1)^{N^2-2}) \\ &= \epsilon N^4 + \beta m' N^4 - \frac{\beta^2 N^4}{2(k+1)}(k+1-1) = N^4(\epsilon + \beta m' - \frac{\beta^2 k^2}{2k(k+1)}) \end{aligned} \tag{55}$$

Equating LHS and RHS,

$$2k(k+1)(k-1)\epsilon = 2k(k+1)\beta m' - \beta^2 k^2, \quad \text{mod N} \tag{56}$$

Using $k(k+1) = -1$ (mod N), $k - 1 = k(k+2)$ (mod N), $\beta = (k+2)m$ (mod N), and $m' = (k+1)m$ (mod N), we find,

$$2k\epsilon = 2(k+1)m^2 + (k+2)m^2k^2 \ \rightarrow 2\epsilon = k^2m^2 = 2\delta \quad \text{mod N} \tag{57}$$

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

Assume $\Delta_\gamma = 0$ and $(1 + k^{N^{\gamma-1}} - (k+1)^{N^{\gamma-1}}) = \delta N^{\gamma+1} + O(N^{\gamma+2})$, we show $\Delta_{\gamma+1} = 0$ 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 (47), (48) and (49) are now,

$$\begin{aligned}
a_{new} \to a &= 1 + (\Delta_{\gamma+1} - \delta)N^{\gamma+1} + \tilde{a}_{\gamma+2}N^{\gamma+2} \qquad (58)\\
b_{new} \to b &= k^{N^{\gamma-1}} + (b_2N^2 + ... + b_{\gamma+1}N^{\gamma+1}) + \tilde{b}_{\gamma+2}N^{\gamma+2} \qquad (59)\\
c_{new} \to c &= -(k+1)^{N^{\gamma-1}} - (b_2N^2 + ... + b_{\gamma+1}N^{\gamma+1}) + \tilde{c}_{\gamma+2}N^{\gamma+2} \qquad (60)
\end{aligned}$$

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

$$\begin{aligned}
a_{new} \to a &= 1 + (\Delta_4 - \delta)N^4 + \tilde{a}_5N^5 \qquad (61)\\
b_{new} \to b &= k^{N^2} + (b_2N^2 + b_3N^3 + b_4N^4) + \tilde{b}_5N^5 \qquad (62)\\
c_{new} \to c &= -(k+1)^{N^2} - (b_2N^2 + b_3N^3 + b_4N^4) + \tilde{c}_5N^5 \qquad (63)
\end{aligned}$$

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,

$$\begin{aligned}
&1 + k^{N^\gamma} - (k+1)^{N^\gamma} = 1 + k^{N^{\gamma-1}}k^{(N-1)N^{\gamma-1}} - (k+1)^{N^\gamma}(k+1)^{(N-1)N^\gamma}\\
=\ & 1 + k^{N^{\gamma-1}}(1+mN)^{N^{\gamma-1}} - (k+1)^{N^\gamma}(1+m'N)^{N^\gamma}\\
=\ & (1 + k^{N^{\gamma-1}} - (k+1)^{N^{\gamma-1}}) + (mk^{N^{\gamma-1}} - m'(k+1)^{N^{\gamma-1}})N^\gamma\\
& + \frac{N^{\gamma+1}(N^{\gamma-1}-1)}{2}(m^2k^{N^{\gamma-1}} - m'^2(k+1)^{N^{\gamma-1}}) + ...\\
=\ & \delta N^{\gamma+1} + (mk^{N^{\gamma-1}} - m'(1 + k^{N^{\gamma-1}} - \delta N^{\gamma+1}))N^\gamma - \frac{N^{\gamma+1}}{2}(m^2 - m'^2) + ...\\
=\ & \delta N^{\gamma+1} + ((m-m')k^{N^{\gamma-1}} - m')N^\gamma + \frac{N^{\gamma+1}}{2}(m'^2(k+1) - m^2k) + ...\\
=\ & \delta N^{\gamma+1} + ((m-m')k(1+mN) - m')N^\gamma + \frac{N^{\gamma+1}}{2}(m'-m)mk + ...\\
=\ & \delta N^{\gamma+1} + ((mk - m'(k+1)) - k^2m^2N)N^\gamma + \frac{N^{\gamma+1}}{2}m^2k^2 + ...\\
=\ & (\delta - \frac{1}{2}k^2m^2)N^{\gamma+1} + ... = 0 \qquad (64)
\end{aligned}$$

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,

$$k^{N^\gamma}(1 + k^{N^\gamma} - (k+1)^{N^\gamma}) = k^{N^\gamma}\epsilon N^{\gamma+2}. \qquad (65)$$

To the order $N^{\gamma+2}$, the RHS of equation (54) is $k\epsilon N^{\gamma+2}$. The LHS is,

$$\begin{aligned} LHS &= k^{N^\gamma} + (k^2)^{N^\gamma} - (k(k+1))^{N^\gamma} = k^{N^\gamma} + (\beta N - (k+1))^{N^\gamma} + (1-\beta N)^{N^\gamma} \\ &= 1 + k^{N^\gamma} - (k+1)^{N^\gamma} + ((k+1)^{N^\gamma - 1} - 1)\beta N^{\gamma+1} \\ &\quad + \frac{1}{2} N^\gamma (N^\gamma - 1)\beta^2 N^2 (1 - (k+1)^{N^\gamma - 2}) \\ &= \epsilon N^{\gamma+2} + \beta m' N^{\gamma+2} - \frac{\beta^2 N^{\gamma+2}}{2(k+1)}(k+1-(k+1)^{N^\gamma - 1}) \\ &= N^{\gamma+2}(\epsilon + \beta m' - \frac{\beta^2 k^2}{2k(k+1)}) \end{aligned} \tag{66}$$

Equating LHS and RHS, we find the same equation (57) 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.

Case II: $N \mid c$ and $N \nmid (ab)$, i. e. N divides one and only one of a,b, and c (choosen here to be c). Let $c = yN^\alpha = (x_0 + x_1 N)N^\alpha$ where $\alpha \geq 1$ and $|x_0| < N$; and let $\gamma = N\alpha - 1$, From Fermat's little theorem, we have

$$a + b + c = (x_0 + x_1' N)N^\alpha \tag{67}$$

Clearly $a + b + c$ is of order N^α. In a similar fashion as in Case I, we can show $\alpha \geq 2$. Consider the auxiliary quantity $\Omega = a^N + (b+c)^N$. We have

$$\Omega = (b+c)^N + a^N = (xN^\alpha - a)^N + a^N = x_0 N^{\alpha+1} + O(N^{\alpha+2}) \tag{68}$$

So its leading term is $x_0 N^{\alpha+1}$.

It is readily shown that,

$$a = \Delta + \tilde{a}_\gamma N^\gamma, \quad b = -\Delta + \tilde{b}_\gamma N^\gamma, \quad c = (c_0 + \tilde{c}_1 N)N^\alpha. \tag{69}$$

where $\gamma = N\alpha - 1$. From the Barlow-Abel relation, we can express $(b+c)$ as r^N. Therefore,

$$\Omega = (r)^{N^2} + a^N = (r_0 + r_1 N)^{N^2} + (a_0 + a_1 N)^N \tag{70}$$

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

$$\begin{aligned}
\Omega &= (r_0 + r_1 N)^{N^2} + (a_0 + a_1 N)^N = -a_0^{N^2} + r_1 N^3 + a_0^N + a_1 N^2 + O(N^3) \\
&= -a_0^N (1 + m_a N^2) + r_1 N^3 + a_0^N + a_1 N^2 + O(N^3) \\
&= (a_1 - m_a a_0) N^2 + O(N^3) \qquad (71)
\end{aligned}$$

If $\alpha = 1$, then we have,

$$(a_1 - m_a a_0) = x_0 \bmod \mathrm{N} \qquad (72)$$

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

$$(b_1 - m_b b_0) = x_0 \bmod \mathrm{N} \qquad (73)$$

where $b_0^{N-1} = 1 + m_b N$ is understood. However, since $a_0 = -b_0$, so $a_0^{N-1} = b_0^{N-1}$, therefore $m_a = m_b \pmod{\mathrm{N}}$. Since $x_0 \neq 0$, equation (72) contradicts with (73) because $a_1 = -b_1$. So α must be larger than 1, and $x_0 = 0$. Equation (72) and (73) now become,

$$(a_1 - m_a a_0) = 0 \bmod \mathrm{N}, \qquad (b_1 - m_b b_0) = 0 \bmod \mathrm{N} \qquad (74)$$

Therefore we have

$$a = a_0^N + \tilde{a}_2 N^2, \quad b = -b_0^N + \tilde{b}_2 N^2, \quad c = (c_0 + \tilde{c}_1 N) N^\alpha \qquad (75)$$

with $\alpha \geq 2$. To further "ascend" α to 3 and beyond, however, can not be done as in Case I.

Discussion

Mr. Fermat is arguably the best amateur mathematician. 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. Note that the proof is not complete for even case I of FLT, because the k^3-conjecture is not proven. So, it could well be that Mr. Fermat had an even better proof. The search goes on.

Acknowledgement: 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 (which now ends). 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 Bejing and Dr. Xudong Sun for his help during my stay in Stanford. I also thank Dr. Yao Chen and Dr. Yong Jiang for their hospitalities 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. Ribenboim, Paulo, *13 lectures on Fermat's last theorem*, Verlag: Springer. (1979).