A proof of Fermat's Last Theorem by modulo operation

H. Tohmori 2021.11.25

Abstract

If Fermat's equation holds in arithmetic operation, it always holds in modulo operation.

But, even if Fermat's equation holds in modulo operation, it does not necessarily hold in arithmetic operation.

However, Fermat's equation never holds in arithmetic operations unless it holds in modulo operation.

Therefore, by proving that Fermat's equation whose exponent is prime p does not hold in modulo operation, it is proved that Fermat's equation does not hold in arithmetic operation.

As a result, Fermat's Last Theorem is proved.

1. At the beginning

Fermat's equation with an exponent of prime p is as follows.

$$A^p + B^p = C^p \qquad (1.1)$$

Following has already been proved conditionally by D.R.Heath-Brown etc.

"If both n and $kn+1$ are prime numbers, Fermat's Last Theorem holds $(k = 2,3,\ldots)$. In addition, there are innumerable prime numbers n such that both n and $kn+1$ are prime numbers."

However, Fermat's Last Theorem for exponent of every prime number has not been proved only using elementary algebra.

$\left(\frac{Q}{R}\right)$ is defined as remainder (modulo) when natural number Q is modulo operated by natural number R.

The notation in the center is correct, but it is written as shown on the right side.

$$\left(\frac{QS}{RT}\right)=\left(\frac{\left(\frac{Q}{RT}\right)\left(\frac{S}{RT}\right)}{RT}\right)=\left(\frac{Q}{RT}\right)\left(\frac{S}{RT}\right) \qquad \left(\frac{Q\pm S}{RT}\right)=\left(\frac{\left(\frac{Q}{RT}\right)\pm\left(\frac{S}{RT}\right)}{RT}\right)=\left(\frac{Q}{RT}\right)\pm\left(\frac{S}{RT}\right)$$

2. Derivation of equation (2.2.3)

2.1 Derivation of equation (2.1.4)

If above Fermat's equation (1.1) holds in arithmetic operation, natural number X and Y that hold below two equations (2.1.1) and (2.1.2) in arithmetic operation exist.

X, Y, B and C are natural number and coprime to each other.

$$X=C^p-B^p \tag{2.1.1}$$

$$Y=C^p+B^p \tag{2.1.2}$$

Then, by multiplying both sides of equations (2.1.1) and (2.1.2), following equation (2.1.3) is created.

$$XY=(C^p-B^p)(C^p+B^p)=C^{2p}-B^{2p}$$

$$XY=C^{2p}-B^{2p}=(C^2-B^2)(\textstyle\sum_{i=1}^{p}C^{2(p-i)}B^{2(i-1)}) \tag{2.1.3}$$

If above equation (2.1.3) holds in arithmetic operation, above equation (2.1.3) must hold in modulo operation by $(2p+1)$. Therefore, following equation (2.1.4) must hold.

$$\left(\frac{XY}{2p+1}\right)=\left(\frac{C^{2p}-B^{2p}}{2p+1}\right)=\left(\frac{C^2-B^2}{2p+1}\right)\left(\frac{\sum_{i=1}^{p}C^{2(p-i)}B^{2(i-1)}}{2p+1}\right) \tag{2.1.4}$$

2.2 Derivation of equation (2.2.3)

Sum part on the right side of the equation (2.1.4) is examined below.

Note that the denominator is $(2p+1)$, not prime number p

$$\left(\frac{\sum_{i=1}^{p}C^{2(p-i)}B^{2(i-1)}}{2p+1}\right)=\sum_{i=1}^{p}\left(\frac{C^{2(p-i)}B^{2(i-1)}}{2p+1}\right)=\sum_{i=1}^{p}\left(\frac{(C^{(p-i)}B^{(i-1)})^2}{2p+1}\right) \tag{2.2.1}$$

$$D=(C^{(p-i)}B^{(i-1)}) \qquad D^2=(C^{(p-i)}B^{(i-1)})^2$$

Number of remainders of D and D^2 in modulo operation by $(2p+1)$ are limited to $2p$ and p as shown below.

$$i=1\sim p$$

$$D:\ 1,\quad 2,\quad 3,\dots\dots\dots,\ p,\quad p+1,\dots,\ p+i\ ,\dots,2p-1,\ 2p$$

$$\left(\frac{D}{2p+1}\right):\left(\frac{1}{2p+1}\right),\left(\frac{2}{2p+1}\right),\left(\frac{3}{2p+1}\right),\dots,\left(\frac{p}{2p+1}\right),\left(\frac{p+1}{2p+1}\right),\dots,\left(\frac{p+i}{2p+1}\right),\dots\left(\frac{2p-1}{2p+1}\right),\left(\frac{2p}{2p+1}\right)$$

$$D^2:1\ ,\ \ 4\ \ ,\ 9\ ,\ \dots\ ,\ p^2\ ,\ (p+1)^2,\dots,(p+i)^2,\dots,(2p-1),\ (2p)^2$$

$$(p+i)^2 = p^2 + 2ip + i^2 = (p-i+1)^2 + (2i-1)(2p+1)$$

$$\left(\frac{(p+i)^2}{2p+1}\right) = \left(\frac{(p-i+1)^2+(2i-1)(2p+1)}{2p+1}\right) = \left(\frac{(p-i+1)^2}{2p+1}\right)$$

$$\left(\frac{D^2}{2p+1}\right) : \left(\frac{1}{2p+1}\right), \left(\frac{4}{2p+1}\right), \left(\frac{9}{2p+1}\right), \dots, \left(\frac{p^2}{2p+1}\right), \left(\frac{(p+1)^2}{2p+1}\right), \dots, \left(\frac{(p+i)^2}{2p+1}\right), \dots, \left(\frac{(2p-1)^2}{2p+1}\right), \left(\frac{(2p)^2}{2p+1}\right)$$

$$\left(\frac{D^2}{2p+1}\right) : \left(\frac{1}{2p+1}\right), \left(\frac{4}{2p+1}\right), \left(\frac{9}{2p+1}\right), \dots, \left(\frac{p^2}{2p+1}\right), \left(\frac{p^2}{2p+1}\right), \dots, \left(\frac{(p-i+1)^2}{2p+1}\right), \dots, \left(\frac{4}{2p+1}\right), \left(\frac{1}{2p+1}\right)$$

As described above, number of remainders(modulo) of D^2 in modulo operation by $(2p+1)$ are limited to p remainders(modulo) shown below.

$$\left(\frac{D^2}{2p+1}\right) : \left(\frac{1}{2p+1}\right), \left(\frac{4}{2p+1}\right), \left(\frac{9}{2p+1}\right), \dots, \left(\frac{j^2}{2p+1}\right), \dots, \left(\frac{(p-2)^2}{2p+1}\right), \left(\frac{(p-1)^2}{2p+1}\right), \left(\frac{p^2}{2p+1}\right) \qquad (2.2.2)$$

Modulo operation (3.1) is the sum of p remainders(modulo) in modulo operation by $(2p+1)$.

Each of those p remainders(modulo) of modulo operation (3.1) always corresponds to one of above p remainders of D^2 in modulo operation by $(2p+1)$. That is, following equation holds.

$$i = 1 \sim p \qquad j = 1 \sim p$$

$$\left(\frac{C^{2(p-i)}B^{2(i-1)}}{2p+1}\right) = \left(\frac{(C^{(p-i)}B^{(i-1)})^2}{2p+1}\right) = \left(\frac{j^2}{2p+1}\right)$$

Therefore, the sum part on the right side of above equation $(2.2.1)$ is rewritten as follows and following equation $(2.2.3)$ holds.

$$\left(\frac{\sum_{i=1}^{p} C^{2(p-i)}B^{2(i-1)}}{2p+1}\right) = \sum_{i=1}^{p}\left(\frac{C^{2(p-i)}B^{2(i-1)}}{2p+1}\right) = \sum_{i=1}^{p}\left(\frac{(C^{(p-i)}B^{(i-1)})^2}{2p+1}\right)$$

$$\sum_{j=1}^{p} j^2 = p(p+1)(2p+1)/6$$

$$= \sum_{j=1}^{p}\left(\frac{j^2}{2p+1}\right) = \left(\frac{\sum_{j=1}^{p} j^2}{2p+1}\right) = \left(\frac{p(p+1)(2p+1)/6}{2p+1}\right)$$

$$\left(\frac{\sum_{i=1}^{p} C^{2(p-i)}B^{2(i-1)}}{2p+1}\right) = \left(\frac{p(p+1)(2p+1)/6}{2p+1}\right) \qquad (2.2.3)$$

Above equation $(2.2.3)$ holds regardless of whether $(2p+1)$ is prime number.

3. Derivation of equation (3.3.3)

3.1 Generation of prime numbers

The formula for the sum of squares of natural numbers is as follows.

$\sum_{i=1}^{k} i^2 = 1 + 2^2 + 3^2 + \cdots + (k-2)^2 + (k-1)^2 + k^2 = k(K+1)(2k+1)/6$

Since the sum of squares of natural numbers is an integer, $k(K+1)(2k+1)$ is divisible by number 6.

When $p_k = 2k+1$ is prime number, $2k+1$ is not divisible by number 6.

At that time, k or $k+1$ is divisible by number 3 because either of them is even number.

As a result, prime number p_k is generated in following two series.

In order to clarify the difference between the two series, it is written as follows.

m is natural number

$k = 3m$ $\qquad$ $p_+ = 6m+1$

$k+1 = 3m$ $\qquad$ $p_- = 6m-1$

Any prime number with number 5 or more is generated as prime number p_+ or prime number p_- of above two series.

3.2 When prime number p is prime number p_+

When prime number p is prime number p_+, above equation (2.2.3) is rewritten as follows.

$$p_+ = 6m+1$$

$$\left(\frac{\sum_{i=1}^{p_+} C^{2(p_+-i)}B^{2(i-1)}}{2p_++1}\right) = \left(\frac{p_+(p_++1)(2p_++1)/6}{2p_++1}\right)$$

$$= \left(\frac{(6m+1)(6m+2)(12m+3)/6}{12m+3}\right)$$

$$= \left(\frac{(6m+1)(3m+1)(4m+1)}{3(4m+1)}\right) \qquad (3.2.1)$$

At this time, right side of equation (2.1.4) is rewritten as follows.

$$\left(\frac{XY}{2p_++1}\right) = \left(\frac{C^{2p_+}-B^{2p_+}}{2p_++1}\right) = \left(\frac{C^2-B^2}{2p_++1}\right)\left(\frac{\sum_{i=1}^{p_+} C^{2(p_+-i)}B^{2(i-1)}}{2p_++1}\right)$$

$$= \left(\frac{C^2-B^2}{3(4m+1)}\right)\left(\frac{(6m+1)(3m+1)(4m+1)}{3(4m+1)}\right)$$

$$= \left(\frac{(C^2-B^2)(6m+1)(3m+1)(4m+1)}{3(4m+1)}\right)$$

$$= \left(\frac{(C^2-B^2)(6m+1)(3m+1)}{3}\right)$$

$$= \left(\frac{C^2-B^2}{3}\right)\left(\frac{6m+1}{3}\right)\left(\frac{3m+1}{3}\right) = 0$$

$$\left(\frac{C^2-B^2}{3}\right) = 0 \qquad \left(\frac{6m+1}{3}\right) = 1 \qquad \left(\frac{3m+1}{3}\right) = 1$$

In other words, when prime number p is prime number p_+, right side of above equation (2.1.4) is 0 regardless of B and C.

3.3 When prime number p is prime number p_-

When prime number p is prime numberp_-, above equation (2.2.3) is rewritten as follows.

$$p_- = 6m - 1$$

$$\left(\frac{\sum_{i=1}^{p_-} C^{2(p-i)}B^{2(i-1)}}{2p_-+1}\right) = \left(\frac{p_-(p_-+1)(2p_-+1)/6}{2p_-+1}\right)$$

$$= \left(\frac{(6m-1)(6m)(12m-1)/6}{12m-1}\right)$$

$$= \left(\frac{(6m-1)(m)(12m-1)}{12m-1}\right) = 0$$

At this time, right side of above equation (2.1.4) is rewritten as follows.

$$\left(\frac{XY}{2p_-+1}\right) = \left(\frac{C^{2p_-}-B^{2p_-}}{2p_-+1}\right) = \left(\frac{C^2-B^2}{2p_-+1}\right)\left(\frac{\sum_{i=1}^{p_-} C^{2(p_--i)}B^{2(i-1)}}{2p_-+1}\right) = 0 \qquad (3.3.1)$$

In other words, when prime number p is prime number p_-, right side of above equation (2.1.4) is 0 regardless of C and B.

As described above, the following equation (3.3.3) holds regardless of C and B.

$$\left(\frac{XY}{2p+1}\right) = \left(\frac{C^{2p}-B^{2p}}{2p+1}\right) = \left(\frac{C^2-B^2}{2p+1}\right)\left(\frac{\sum_{i=1}^{p} C^{2(p-i)}B^{2(i-1)}}{2p+1}\right) = 0 \qquad (3.3.3)$$

4. Fermat's equation (1.1)

4.1 When neither natural numbers C and B contains factor $(2p+1)$

From the equation (3.3.3) in the previous section, either of the following equations (4.1.1) or (4.1.2) holds.

$$\left(\frac{X}{2p+1}\right) = 0 \qquad (4.1.1)$$

$$\left(\frac{Y}{2p+1}\right) = 0 \qquad (4.1.2)$$

When equation (4.1.2) holds, equation (4.1.3) holds as shown below.

$$\left(\frac{Y}{2p+1}\right) = \left(\frac{C^p+B^p}{2p+1}\right) = \left(\frac{C^p}{2p+1}\right) + \left(\frac{B^p}{2p+1}\right) = 0$$

$$\left(\frac{C^p}{2p+1}\right) = -\left(\frac{B^p}{2p+1}\right)$$

$$\left(\frac{X}{2p+1}\right) = \left(\frac{C^p-B^p}{2p+1}\right) = \left(\frac{2C^p}{2p+1}\right) \qquad (4.1.3)$$

Therefore, in order for Fermat's equation (1.1) to hold, the following equation (4.1.4) must hold.

$$\left(\frac{A^p}{2p+1}\right) = \left(\frac{X}{2p+1}\right) = \left(\frac{2C^p}{2p+1}\right)$$

$$A^p = 2C^p \qquad (4.1.4)$$

However, there is no natural number A that holds above equation.

Therefore, there are no natural numbers A, B and C that hold Fermat's equation (1.1).

4.2 When neither natural number A and B contain factor $(2p+1)$

There is always natural number U and V that holds following equations (4.2.1) and (4.2.2).

$$A^p - B^p = U \qquad (4.2.1)$$

$$A^p + B^p = V = C^p \qquad (4.2.2)$$

Similar to previous section 4.1, either of following equations (4.2.3) or (4.2.4) hold.

$$\left(\frac{U}{2p+1}\right) = 0 \qquad (4.2.3)$$

$$\left(\frac{V}{2p+1}\right) = 0 \qquad (4.2.4)$$

When the above equation (4.2.3) holds, the following equation (4.2.5) must hold, as shown below.

$$\left(\frac{U}{2p+1}\right) = \left(\frac{A^p - B^p}{2p+1}\right) = \left(\frac{A^p}{2p+1}\right) - \left(\frac{B^p}{2p+1}\right) = 0$$

$$\left(\frac{A^p}{2p+1}\right) = \left(\frac{B^p}{2p+1}\right)$$

$$\left(\frac{V}{2p+1}\right) = \left(\frac{A^p + B^p}{2p+1}\right) = \left(\frac{2A^p}{2p+1}\right) \qquad (4.2.5)$$

Therefore, in order for Fermat's equation (1.1) to hold, the following equation (4.2.6) must hold.

$$\left(\frac{C^p}{2p+1}\right) = \left(\frac{V}{2p+1}\right) = \left(\frac{2A^p}{2p+1}\right)$$

$$C^p = 2A^p \qquad (4.2.6)$$

However, there are no natural numbers C that hold above equation (4.2.6).

As above, when exponent is prime number p, Fermat's Last Theorem holds.

5. Conclusion

Fermat's equation with an exponent of prime p does not hold in the modulo operation.

Therefore, there are no natural numbers A, B and C that hold Fermat's equation with an exponent of prime p.

Then, Fermat's Last Theorem holds.

6. References

[1] L. Riddle, "Sophie Germain and Fermat's Last Theorem," Agnes Scott College, 2009.
http://www.agnesscott.edu/Lriddle/women/germain-

FLT/SGandFLT.htm

[2] Colleen-Alkalay-Houlihan, “Sophie Germain and Special Cases of Fermat’s Last Theorem”

https://www.math.mcgill.ca/darmon/courses/12-13/nt/projects/Colleen-Alkalay-Houlihan.pdf

[3] B. B. U. Perera, R. A. D. Piyadasa “Proof of Fermat’s Last Theorem for n = 3 Using Tschirnhaus Transformation” 2016

https://link.springer.com/chapter/10.5176/2251-1911_CMCGS14.34_12#citeas

[4] Kunle Oladeji Babalola “A simple proof of the fermat’s last theorem” 2010

https://www.researchgate.net/profile/Kunle-Oladeji-Babalola/publication/328164214_A_SIMPLE_PROOF_OF_THE_FERMAT'S_LAST_THEOREM/links/5bbc92f792851c7fde372fa6/A-SIMPLE-PROOF-OF-THE-FERMATS-LAST-THEOREM.pdf

[5] Piyadasa, R.A.D. “A simple analytical proof of Fermat’s last theorem for n = 7” 2010

http://repository.kln.ac.lk/handle/123456789/4753

[6] C.U.Ubeynarayana, R.A.D. Piyadasa, & J.Munasinghe “Roots of a cubic and simple proof of Fermat's last theorem for n=3” 2013

https://www.researchgate.net/publication/343282033

[7] Zhang Yue “A simple proof on Fermat’s last theorem in case of n=3” 2020

https://www.mathematicaljournal.com/article/9/1-1-17-231.pdf

[8] P. N. Seetharaman “A Proof of Fermat’s Last Theorem using an Euler’s equation” 2017

[9] Youngik Lee “Numerical Approach for Fermat’s last theorem” 2019

https://arxiv.org/pdf/1912.04046.pdf

[10] Kaida Shi “The n-Dimensional Cube---A New Approach to Prove Fermat's Last Theorem” 2010

https://www.researchgate.net/profile/Kaida-Shi-2/publication/2108398_The_n-dimensional_Cube--

A_New_Way_to_Prove_the_Fermat's_Last_Theorem/links/5f6fc453a6fdcc00863e154f/The-n-dimensional-Cube--A-New-Way-to-Prove-the-Fermats-Last-Theorem.pdf

[11] John Sherrill “An Elementary Proof of Fermat’s Last Theorem” 2017

http://www.sciencepublishinggroup.com/j/ml

[12] M.Meyyappan “Resolving Fermat’s Last Theorem by Prime Factor Method and Proof in 5 steps” 2017

http://www.ijmttjournal.org/2017/Volume-46/number-1/IJMTT-V46P510.pdf

[13] Vinay Kumar “Proof of Beal's conjecture and Fermat last theorem using contra positive method” 2018

https://www.researchgate.net/publication/326630714

[14] Bhupinder Singh Anand “An Elementary Pre-formal Proof of FLT” 2021

https://philarchive.org/archive/ANAAEPv2

[15] Mollin R.A. “How to prove Fermat's last theorem” 2009

https://www.scopus.com/home.uri

[16] Dora Musielak “Germain and Her Fearless Attempt to Prove Fermat’s Last Theorem” 2020

https://arxiv.org/pdf/1904.03553.pdf

[17] X. S. Zhang “Fermat's last theorem proved by a simple method” 1991

https://www.sciencedirect.com/science/article/abs/pii/0013794491900394?via%3Dihub

[18] D.R. Heath-Brown and L.M. Adleman “The first case of Fermat's last theorem” June 1985Inventiones mathematicae 79(2):409-416

http://eudml.org/doc/143203