剰余演算を用いたフェルマーの最終定理の証明

東森秀朋　2021.11.26

要約

フェルマーの等式は，算術演算において成立するならば，剰余演算において必ず成立する．しかし、フェルマーの等式は，剰余演算において成立しても，算術演算において必ずしも成立しない．ただ，フェルマーの等式は，剰余演算において成立しないならば，算術演算において決して成立しない．

そこで，指数が素数pのフェルマーの等式が算術演算において成立しないことを証明するために，指数が素数pのフェルマーの等式が剰余演算において成立しないことを証明する．

この証明により，指数が素数pのフェルマーの等式を算術演算において成立させる自然数A，BおよびCは存在しないことが証明される．

1．始めに

指数が素数pのフェルマーの等式は次のとおりである．

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

次のことはヒース・ブラウン等により既に証明されている．

“指数pと$kp+1$が共に素数であるならば，フェルマーの最終定理は成立する$(k = 2, 3, \ldots)$．また，nと$kn+1$が共に素数である素数は無数に存在する．”

しかしながら，あらゆる素数pの指数に対してフェルマーの最終定理の初等代数学のみを用いた証明はなされていない．

自然数A，B及びCは互いに素である．

$\left(\frac{Q}{R}\right)$は自然数Qを自然数Rで剰余演算したときの剰余である．

中央の表記が正しいが，右辺のように表記する．

自然数R　自然数S

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

2.　等式 (2.2.3)の導出

2.1　等式(2.1.3)の導出

フェルマーの等式(1.1)が算術演算において成立するならば，指数が素数pの２

個の等式(2.1.1)及び(2.1.2)を算術演算において成立させる自然数X，Yは必ず存在する．

自然数X，Y，B及びCは互いに素である．B及びCは因子$(2p+1)$を含まない．

$$X = C^p - B^p \qquad (2.1.1)$$

$$Y = C^p + B^p \qquad (2.1.2)$$

上記等式(2.2)と等式(2.3)の両辺を乗算すると，次の等式(2.1.3)が成立する．

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

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

上記等式(2.1.3)は，算術演算において成立するから，因子$(2p+1)$による剰余演算において成立しなければならない．それ故，次の等式(2.1.4)が成立しなければならない．

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

2.2　等式(2.2.3)の導出

等式(2.1.4)の右辺の剰余演算の総和部分について以下に検討する．

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

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

因子$(2p+1)$による剰余演算におけるD及びD^2の剰余は以下に示すようにそれぞれ$2p$個とp個に限られる．

C ： 1　2　3 …… p　$p+1$ …… $p+i$ …… $2p$

C^2 : 1　4　9 …　p^2　$(p+1)^2$ …　$(p+i)^2$ …… $(2p)^2$

$i = 1 \sim p$

D ： 1,　2 ,　3, …… , p,　$p+1$, … , $p+i$, … , $2p-1$,　$2p$

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

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

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

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

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

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

以上のとおり，因子$(2p+1)$による剰余演算におけるD^2の剰余は以下に示すp

個に限られる．

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

上記等式(2.2.1)の右辺は，因子 $(2p+1)$による剰余演算におけるp個の剰余の総和である．そのp個の剰余の各々は上記D^2のp個の剰余(2.2.2)の何れかに必ず一致する．即ち，次の等式が成立する．

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

それ故，上記等式(2.2.1)の右辺の総和は以下の如く書き換えられ，以下の等式(2.2.3)が成立する．

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

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

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

以上のとおり，pは素数であるが，$(2p+1)$が素数であるか否かに関係しないで，下記等式(2.2.3)は成立する．

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

3. 等式 (3.3.3)の導出

3.1 素数の生成

自然数の２乗和の公式は次のとおりである．

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

自然数の２乗和は整数であるから，$k(K+1)(2k+1)$は数6で割り切れる．

$p_k = 2k+1$が数5以上の素数であるとき，$(2k+1)$は数6で割り切れない．

そのとき，kまたは$k+1$は，いずれかは偶数であるから，数3の倍数である．

その結果，素数p_kは次の２系列で生成される．

２系列の相違を明確にするため，以下のように表記する．

mは自然数

$k = 3m$　　$p_+ = 6m+1$

$k+1 = 3m$　　$p_- = 6m-1$

表記から判るように，素数5以上のあらゆる素数は上記２系列の素数p_+または素数p_-として生成される．

3.2　素数pが素数p_+のとき

素数pが素数p_+のとき，上記等式(2.2.3)は次の等式(3.2.1)に書き換えられる．

$$p_+ = 6m+1$$

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

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

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

そして，上記等式(2.1.4)は上記等式(3.2.1)を用いて次のように書き換えられる．

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

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

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

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

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

自然数B及びCは，因子$(2p+1)$と互いに素であるから，数 3 を含まない．

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

つまり，素数pが素数p_+のとき，上記等式(2.1.4)の右辺は，B及びCの如何に関わらず，上記のように零0に等しい．

3.3　素数pが素数p_-のとき

素数pが素数p_-のとき，上記等式(2.2.3)は次のように書き換えられる．

$$p_- = 6m-1$$

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

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

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

上記等式(3.2.1)を用いて上記等式(2.1.4)は次の等式(3.3.2)に書き換えられる．

$$\left(\frac{XY}{2p_-+1}\right)=\left(\frac{C^{2p_-}-B^{2p_-}}{2p_-+1}\right)=\left(\frac{C^2-B^2}{2p_-+1}\right)\left(\frac{\sum_{i=1}^{p_-}C^{2(p_--i)}B^{2(i-1)}}{2p_-+1}\right)=0 \qquad (3.3.2)$$

つまり，素数pが素数p_-のとき，上記等式(2.1.4)の右辺は，B及びCの如何に関わらず，零0に等しい.

以上のとおり，B及びCの如何に関わらず，次の等式(3.3.3)が成立する.

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

4. フェルマーの等式(1.1)について

4.1 自然数C及びBのどちらも因子$(2p+1)$を含まないとき

前節の等式(3.3.3)からして，次の等式(4.1.1)又は(4.1.2)の何れかが成立する.

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

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

上記等式(4.1.2)が成立するとき，以下に示すように，下記等式(4.1.3)が成立しなければならない.

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

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

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

したがって，フェルマーの等式(1.1)が成立するためには次の等式(4.1.4)が成立しなければならない.

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

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

しかしながら，上記等式(4.1.4)を成立させる自然数Aは存在しない.

4.2 自然数A及びBのどちらも因子$(2p+1)$を含まないとき

次の等式(4.2.1)及び(4.2.2)を成立させる自然数U及びVは必ず存在する.

自然数U，V，A及びBは互いに素である.

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

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

前節 4.1 と同様に，次の等式(4.2.3)又は(4.2.4)の何れかが成立しなければならない．

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

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

上記等式(4.2.3)が成立するとき，以下に示すように，下記等式(4.2.5)が成立しなければならない．

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

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

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

したがって，フェルマーの等式(1.1)が成立するためには次の等式(4.2.6)が成立しなければならない．

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

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

しかしながら，上記等式(4.2.6)を成立させる自然数Cは存在しない．

以上のとおり，指数が素数pのフェルマーの等式(1.1)を成立させる自然数A，B及びCは存在しないから，フェルマーの最後定理は成立する

5. 結論

フェルマーの等式は，算術演算において成立するならば，剰余演算において必ず成立する．しかし、フェルマーの等式は，剰余演算において成立しても，算術演算において必ずしも成立しない．ただ，フェルマーの等式は，剰余演算において成立しないならば，算術演算において決して成立しない．

それ故，指数が素数pのフェルマーの等式は剰余演算において成立しないことを証明することにより，指数が素数pのフェルマーの等式を算術演算において成立させる自然数A，BおよびCは存在しないことが証明された．

6. 参考文献

[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