ソフィー.ジェルマン素数p_sとフェルマーの最終定理

東森秀朋　2021.11.09

要約

ソフィー.ジェルマンは，フェルマーの最終定理(ＦＬＴ)それ自体を証明したのではなく，ＦＬＴが成立するための条件について素数p_sと素数$(2p_s+1)$を用いて研究しました．しかし，指数が素数p_sのフェルマーの等式にはＦＬＴが成立することをソフィー.ジェルマン当時の代数学により証明できました．以下はその概要です.

指数が素数p_sのフェルマーの等式は，算術演算において成立するならば，素数$(2p_s+1)$による剰余演算において必ず成立する．しかし、そのフェルマーの等式は，素数$(2p_s+1)$による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，そのフェルマーの等式は，素数$(2p_s+1)$による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，そのフェルマーの等式は素数$(2p_s+1)$による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，そのフェルマーの等式は算術演算において成立しないことを証明する.

結果として，指数が素数p_sのフェルマーの等式に対するＦＬＴの成立が証明される.

１．始めに

指数が素数p_sのフェルマーの等式は次のとおりである.

$$A^{p_s}+B^{p_s}=C^{p_s} \tag{1.1}$$

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.　素数$(2p_s+1)$による剰余演算の相補性

下記の 2 個の素数$(2p_s+1)$による剰余演算は互いに相補的である.

自然数X，Y，B及びCは互いに素である．

自然数B及びCのいずれも素数$(2p_s+1)$を含まない．

$$X = C^{p_s} - B^{p_s} \qquad Y = C^{p_s} + B^{p_s}$$

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

即ち，以下に示すように，一方の等式が成立しないときは他方の等式が成立する．

$$\left(\frac{C^{2p_s}}{2p_s+1}\right) = \left(\frac{C^{p_s}}{2p_s+1}\right)^2 = 1 \quad \left(\frac{C^{p_s}}{2p_s+1}\right) = \pm 1 \qquad \left(\frac{B^{2p_s}}{2p_s+1}\right) = \left(\frac{B^{p_s}}{2p_s+1}\right)^2 = 1 \quad \left(\frac{B^{p_s}}{2p_s+1}\right) = \pm 1$$

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

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

$$\left(\frac{C^{p_s}+B^{p_s}}{2p_s+1}\right) \neq 0$$

$$\left(\frac{C^{p_s}}{2p_s+1}\right) \neq \left(\frac{B^{p_s}}{2p_s+1}\right)$$

$$\left(\frac{C^{p_s}-B^{p_s}}{2p_s+1}\right) = \left(\frac{C^{p_s}}{2p_s+1}\right) - \left(\frac{B^{p_s}}{2p_s+1}\right) \neq 0$$

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

上記から判るように，自然数B及びCのいずれも素数$(2p_s+1)$を含まないとき，次の等式(2.1)は，自然数C及びBの如何に関わらず，成立する．

$$\left(\frac{XY}{2p_s+1}\right) = \left(\frac{X}{2p_s+1}\right)\left(\frac{Y}{2p_s+1}\right) = \left(\frac{C^{p_s}-B^{p_s}}{2p_s+1}\right)\left(\frac{C^{p_s}+B^{p_s}}{2p_s+1}\right) = \left(\frac{C^{2p_s}-B^{2p_s}}{2p_s+1}\right) = 0 \qquad (2.1)$$

3. 指数が素数p_sのフェルマーの等式

3.1 自然数C及びBのどちらも素数$(2p_s+1)$を含まないとき

上記等式(1.1)は次の等式(3.1.1)に書き換えられる．

そのとき，下記等式(3.1.1)及び(3.1.2)を成立させる自然数X及びYは必ず存在する．

前節の等式(2.1)からして，自然数X及びYのいずれかは素数$(2p_s+1)$を含む．

自然数X，Y，B及びCは互いに素である．

自然数B及びCは素数$(2p_s+1)$を含まない．

$$A^{p_s} = X = C^{p_s} - B^{p_s} \qquad (3.1.1)$$

$$Y = C^{p_s} + B^{p_s} \tag{3.1.2}$$

自然数Yが素数$(2p_s + 1)$を含むとき，以下に示すように，等式(3.1.3)が成立しなければならない.

$$\left(\frac{Y}{2p_s+1}\right) = 0$$

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

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

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

自然数X及びCは互いに素であるから，上記等式が成立するためには，次の等式(3.1.3)が成立しなければならない.

自然数EはCと互いに素である.

$$X = 2E^{p_s} \tag{3.1.3}$$

反対に，自然数X，即ち，自然数Eが素数$(2p_s + 1)$を含むとき，以下に示すように，下記等式(3.1.4)が成立しなければならない.

$$\left(\frac{X}{2p_s+1}\right) = 0$$

$$\left(\frac{X}{2p_s+1}\right) = \left(\frac{C^{p_s}-B^{p_s}}{2p_s+1}\right) = \left(\frac{C^{p_s}}{2p_s+1}\right) - \left(\frac{B^{p_s}}{2p_s+1}\right) = 0$$

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

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

自然数Y及びCは互いに素であるから，上記等式が成立するためには，次の等式(3.1.4)が成立しなければならない.

自然数F，E，C及びBは互いに素である.

自然数F及びEのいずれかは素数$(2p + 1)$を含む.

$$Y = 2F^{p_s} \tag{3.1.4}$$

以上のことから，等式(3.1.1)及び(3.1.2)は次の等式(3.1.5)及び(3.1.6)に書き換えられる.

$$2E^{p_s} = C^{p_s} - B^{p_s} \tag{3.1.5}$$

$$2F^{p_s} = C^{p_s} + B^{p_s} \tag{3.1.6}$$

そうすると，指数が素数p_sのフェルマーの等式(1.1)が成立するためには次の等式が成立しなければならない.

$$A^{p_s} = X = 2E^{p_s} = C^{p_s} - B^{p_s}$$

しかしながら，上記等式を成立させる自然数Aは存在しない．

したがって，自然数C及びBのいずれも素数$(2p_s + 1)$を含まないとき，指数が素数p_sのフェルマーの等式(1.1)を成立させる自然数A，BおよびCは存在しない．

3.2　自然数A及びBのいずれも素数$(2p_s + 1)$を含まないとき

次の等式$(3.2.1)$及び$(3.2.2)$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．

$$A^{p_s} - B^{p_s} = U \qquad (3.2.1)$$

$$A^{p_s} + B^{p_s} = V = C^{p_s} \qquad (3.2.2)$$

前節 3.1 と同様に，次の等式$(3.2.3)$及び$(3.2.4)$が成立する．

自然数G，H，A及びBは互いに素である．

自然数A及びBのいずれも素数$(2p_s + 1)$を含まない．

自然数G及びHのいずれかは素数$(2p + 1)$を含む．

$$A^{p_s} - B^{p_s} = 2G^{p_s} = U \qquad (3.2.3)$$

$$A^{p_s} + B^{p_s} = 2H^{p_s} = V \qquad (3.2.4)$$

そうすると，指数が素数p_sのフェルマーの等式(1.1)が成立するためには次の等式が成立しなければならない．

$$A^{p_s} + B^{p_s} = 2H^{p_s} = V = C^{p_s}$$

しかしながら，上記等式を成立させる自然数Cは存在しない．

したがって，自然数A及びBのいずれも素数$(2p_s + 1)$を含まないとき，指数が素数p_s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．

以上のとおり，指数が素数p_s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．

4.　結論

指数が素数p_sのフェルマーの等式は素数$(2p_s + 1)$による剰余演算において成立しないから，その指数が素数p_sのフェルマーの等式は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_sのフェルマーの等式を成立させる自然数A，B及びCは存在しない．

よって，指数が素数p_sのフェルマーの等式に対してフェルマーの最後定理は証明された．

５． 参考文献

1. https://www.math.uci.edu/~ndonalds/math180b/6germain.pdf.

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

[1] “Sophie Germain.” Encyclopaedia Britannica Online. Encyclopaedia Britannica Inc., 2013.
Web.
http://www.britannica.com/EBchecked/topic/230626/SophieGermain/2647/Additional-Reading.
[2] L. L. Bucciarelli and N. Dworsky, “Sophie Germain,” Studies in the History of Modern Science,
Volume 6, pp. 9-19, 1980.
[3] R.Laubenbacherand D. Pengelley, “‘Voici ce que jai trouv´e:’ Sophie Germain’s grand plan to
prove Fermat’s Last Theorem,” pre-print, 2010.
[4] L. Riddle, “Sophie Germain and Fermat’s Last Theorem,” Agnes Scott College, 2009.
http://www.agnesscott.edu/Lriddle/women/germain-FLT/SGandFLT.htm
[5] S. Singh, excerpt from “Fermat’s Enigma: The Epic Quest to Solve the World’s Greatest Mathematical Problem,” October 1997,
http://www.pbs.org/wgbh/nova/physics/sophiegermain.html.
[6] A. Wiles, “Modular Elliptic Curves and Fermat’s Last Theorem,” Annals of Mathematics,
Second Series, Vol. 141, No. 3, pp. 443-551, May, 1995.

https://www.math.uci.edu/~ndonalds/math180b/6germain.pdf.

References

[1] Andrea Del Centina, Unpublished manuscripts of Sophie Germain and a revaluation of her
work on Fermat's last theorem, Arch. Hist. Exact Sci. 62 (2008), no. 4, 349–392. MR2415091

[2] Jeremy B. Dibbell, Ex Libri, Fine Books & Collections, April, 2010.

[3] Leonard Eugene Dickson, History of the Theory of Numbers, Vol. II: Diophantine Analysis,
American Mathematical Society, Providence, 1999, pp. iv–v, 3–24. MR0245500

[4] Ioan James, Remarkable Mathematicians: From Euler to von Neumann, MAA Spectrum,
Mathematical Association of America, Washington, DC, and Cambridge University Press,
Cambridge, 2002, pp. 47–58. MR1964301

[5] Reinhard Laubenbacher and David Pengelley, "Voici que j'ai trouv´e:" Sophie Germain's
grand plan to prove Fermat's Last Theorem, Hist. Math. 37 (2010) 641–692. MR1964301

[6] Guglielmo Libri, Notice sur Mlle Sophie Germain, Journal des D´ebats, 18 May 1832.

[7] DoraMusielak, Sophie's Diary/A Mathematical Novel, Mathematical Association of America,
Washington, DC, 2012.