フェルマー最終定理の簡潔な証明

東森秀朋　2020.05.16

要約

フェルマー最終定理の等式$A^n + B^n = C^n$（以下、フェルマーの等式）が四則演算において成立するならば，素因数p_kによる剰余演算においても成立する．しかし、フェルマーの等式は素因数p_kの剰余演算において成立しても，四則演算においては必ずしも成立しない．ただ，素因数p_kの剰余演算においてフェルマーの等式が成立しないならば，四則演算においても決して成立しない．そこで，素因数p_kによる剰余演算において自然数A，B及びCに依存しないで(の如何に関わらず)フェルマーの等式が成立するための必要十分条件を求める．その自然数A，B及びCには四則演算においてフェルマーの等式を成立させる自然数A_a，B_a及びC_aも含まれる．その自然数A_aに含まれる素因数$p_j \neq p_k$による剰余演算においてもフェルマーの等式は成立する．このことから$n = 2$が証明される．

１．始めに

フェルマーの最終定理は“指数$\mathrm{n} > 2$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”というものである．

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

自然数A，B及びCは，それぞれ互いに異なる素因数の累乗の積に分解される．素因数2はAまたはBに含まれる．自然数A，B及びCは共通の素因数を含まない．

$\mathrm{Re}\left(\frac{A^n}{p_k}\right)$は$A^n$を素因数$p_k$で剰余演算したときの剰余である．

２．証明方法

フェルマー最終定理の等式$A^n + B^n = C^n$（以下，フェルマーの等式）が四則演算において成立するならば、フェルマーの等式は素因数$p_k = 2k + 1$の剰余演算において成立する．しかし，フェルマーの等式が素因数p_kの剰余演算において成立しても四則演算においては必ずしも成立しない．ただ，フェルマーの等式は素因数p_kによる剰余演算において成立しないならば，四則演算において決して成立しない．そこで，素因数p_kによる剰余演算において自然数A，B及びCに依存しないでフェルマーの等式が成立する必要十分条件を求める．そのとき，その必要十分条件は自然数A，B及びCに依存しないから，その自然数A，B及びCには四

則演算において成立させる自然数A_a，B_a及びC_aも含まれる．四則演算において成立するフェルマーの等式は素因数$p_j \neq p_k$による剰余演算においても成立する．このことから$n = 2$が証明される．

3．必要十分条件

3.1 必要条件

フェルマーの等式(1.1)の両辺を素因数$p_k = 2k + 1$（kは$2k + 1$が素因数である正の整数）によって剰余演算すると，次の等式(3.1) が成立する．

$$\mathrm{Re}\left(\frac{A^n+B^n}{p_k}\right) = \mathrm{Re}\left(\frac{A^{\mathrm{n}}}{p_k}\right) + \mathrm{Re}\left(\frac{B^{\mathrm{n}}}{p_k}\right) = \mathrm{Re}\left(\frac{C^n}{p_k}\right) \qquad (3.1)$$

自然数A，B及びCに依存しないで上記等式(3.1)が成立するためには，指数nは$2k$を含む（即ち，$n = 2km$（mは正の整数））必要があり，素因数p_kは自然数A又はBのいずれかに含まれる必要がある．

3.2 十分条件

必要条件を満たすフェルマーの等式(1.1)の両辺を素因数p_kで剰余演算すると、自然数A、B及びCに依存しないで(の如何に関係なく)次の等式(3.2)が成立する．

$$\mathrm{Re}\left(\frac{A^{2km}+B^{2km}}{p_k}\right) = \mathrm{Re}\left(\frac{A^{2km}}{p_k}\right) + \mathrm{Re}\left(\frac{B^{2km}}{p_k}\right) = \mathrm{Re}\left(\frac{C^{2km}}{p_k}\right) \qquad (3.2)$$

指数nは$2km$（mは正の整数）であり，素因数p_kは自然数A又はBのいずれかに含まれるから，自然数A、B及びCに依存しないで(の如何に関係なく)次の等式(3.3)が成立する．

$$\mathrm{Re}\left(\frac{A^{2km}}{p_k}\right) + \mathrm{Re}\left(\frac{B^{2km}}{p_k}\right) = 1 = \mathrm{Re}\left(\frac{C^{2km}}{p_k}\right) \qquad (3.3)$$

以上のとおり，必要条件は十分条件でもある．

自然数A, B及びC(の如何に関係なく)に依存しないで等式(3.3)は成立するから，その自然数A, B及びCには，四則演算においてフェルマーの等式を成立させる自然数A_a，B_a及びC_aも含まれる．つまり，四則演算において成立するフェルマーの等式の指数nは$2km$である．

4．$n = 2$の証明

必要十分条件を満たすフェルマーの等式は次のとおりである．

$$A^{2km} + B^{2km} = C^{2km} \qquad (4.1)$$

そうすると，以下に示すように等式(4.2)が成立する．

$$A^{2km} = C^{2km} - B^{2km}$$
$$= (C^{2k} - B^{2k})(C^{2k(m-1)} + C^{2k(m-2)}B^{2k} + C^{2k(m-3)}B^{4k} + \cdots + C^{2k}B^{2k(m-2)} + B^{2k(m-1)})$$
$$A^{2km} = (C^2 - B^2)(C^{2(k-1)} + C^{2(k-2)}B^2 + C^{2(k-3)}B^4 + \cdots + C^2B^{2(k-2)} + B^{2(k-1)})(C^{2k(m-1)} + C^{2k(m-2)}B^{2k} + C^{2k(m-3)}B^{4k} + \cdots + C^{2k}B^{2k(m-2)} + B^{2k(m-1)})$$
$$A^{2km} = (C^2 - B^2)(\sum_{i=1}^{k} C^{2(k-i)}B^{2(i-1)})(\sum_{i=1}^{m} C^{2k(m-i)}B^{2k(i-1)}) \qquad (4.2)$$

上記等式(4.2)の両辺をAに含まれる素因数p_kによって剰余演算をすると，次の等式(4.3)が成立する．

$$\mathrm{Re}\left(\frac{A^{2km}}{p_k}\right) = \mathrm{Re}\left(\frac{(C^2-B^2)(\sum_{i=1}^{k} C^{2(k-i)}B^{2(i-1)})(\sum_{i=1}^{k} C^{2k(m-i)}B^{2k(i-1)})}{p_k}\right)$$
$$\mathrm{Re}\left(\frac{A^{2km}}{p_k}\right) = \mathrm{Re}\left(\frac{C^2-B^2}{p_k}\right)\mathrm{Re}\left(\frac{\sum_{i=1}^{k} C^{2(k-i)}B^{2(i-1)}}{p_k}\right)\mathrm{Re}\left(\frac{\sum_{i=1}^{k} C^{2k(m-i)}B^{2k(i-1)}}{p_k}\right) \qquad (4.3)$$

素因数p_kは自然数Aに含まれるから，等式(4.3)の左辺の$\mathrm{Re}\left(\frac{A^{2km}}{p_k}\right)$は$m$に依存しないで（の如何に関わらずに）0である．そうすると，mに依存しないで（の如何に関わらずに）右辺も0である．それ故，次の等式(4.4)が成立する．

$$\mathrm{Re}\left(\frac{C^2-B^2}{p_k}\right)\mathrm{Re}\left(\frac{\sum_{i=1}^{k} C^{2(k-i)}B^{2(i-1)}}{p_k}\right) = 0 \qquad (4.4)$$

したがって，自然数C及びBに依存しないで（の如何に関わらずに）次の等式(4.5)及び(4.6)が成立する．

$$p_k = 3 \qquad \mathrm{Re}\left(\frac{C^2-B^2}{p_k}\right) = 0 \qquad (4.5)$$

$$p_k \neq 3 \qquad \mathrm{Re}\left(\frac{\sum_{i=1}^{k} C^{2(k-i)}B^{2(i-1)}}{p_k}\right) = 0 \qquad (4.6)$$

自然数A，B及びCに依存しないで等式(4.2)は成立するから，その自然数A，B及びCには，四則演算において等式(4.2)を成立させる自然数A_a，B_a及びC_aも含まれる．つまり，四則演算において成立するフェルマーの等式の指数nは$2km$である．四則演算において等式(4.2)が成立するとき，自然数A_aに含まれる素因数$p_j = 2j + 1 \neq p_k$（即ち，$j \neq k$，指数nは$2j$を含まない）による等式(4.2)の剰余演算において次の等式が成立する．

$$\mathrm{Re}\left(\frac{{A_a}^{2km}}{p_j}\right) = \mathrm{Re}\left(\frac{{C_a}^2-{B_a}^2}{p_j}\right)\mathrm{Re}\left(\frac{\sum_{i=1}^{k} {C_a}^{2(k-i)}{B_a}^{2(i-1)}}{p_j}\right)\mathrm{Re}\left(\frac{\sum_{i=1}^{k} {C_a}^{2k(m-i)}{B_a}^{2k(i-1)}}{p_j}\right) = 0$$

左辺の$\mathrm{Re}\left(\frac{{A_a}^{2km}}{p_j}\right)$は$m$に依存しないで（の如何に関わらずに）0であるから，右辺もmに依存しないで（の如何に関わらずに）0である．その結果，次の等式(4.7)が成立する．

$$\mathrm{Re}\left(\frac{{A_a}^{2km}}{p_j}\right)=\mathrm{Re}\left(\frac{{C_a}^2-{B_a}^2}{p_j}\right)\mathrm{Re}\left(\frac{\sum_{i=1}^{k}{C_a}^{2(k-i)}{B_a}^{2(i-1)}}{p_j}\right)=0 \qquad (4.7)$$

ところが，等式(4.6)は，四則演算において等式(4.2)を成立させる自然数C_a及びB_a（の如何に関わらずに）に依存しないで，素因数p_kによる剰余演算においてのみ成立する．それ故，素因数$p_j=2j+1\neq p_k$（即ち，$j\neq k$，指数nは$2j$を含まない）による剰余演算において等式(4.6)は成立しない．即ち，次の不等式が成立する．

$$\mathrm{Re}\left(\frac{\sum_{i=1}^{k}{C_a}^{2(k-i)}{B_a}^{2(i-1)}}{p_j}\right)\neq 0$$

そうすると，四則演算において等式(4.2)を成立させる自然数C_a及びB_aに対して次の等式(4.8)が成立しなければならない．

$$p_j\neq 3 \quad p_j\neq p_k \qquad \mathrm{Re}\left(\frac{{C_a}^2-{B_a}^2}{p_j}\right)=0 \qquad (4.8)$$

以上のとおり，$n=2$のみであることは明らかである．

5． 結論

自然数Aに含まれる素因数p_kによる剰余演算において，必要十分条件を備えたフェルマーの等式は自然数A、B及びCに依存しないで成立する．その自然数A，B及びCには，四則演算においてフェルマーの等式を成立させる自然数A_a，B_a及びC_aも含まれる．四則演算で成立するフェルマーの等式はその自然数A_aに含まれる素因数$p_{j\neq}p_k$による剰余演算において成立することから，指数$n=2$が証明された．

6． 補遺１

等式(4.4)について検討する．

$$\mathrm{Re}\left(\frac{C^{2k}-B^{2k}}{p_k}\right)=\mathrm{Re}\left(\frac{C^2-B^2}{p_k}\right)\mathrm{Re}\left(\frac{\sum_{i=1}^{k}C^{2(k-i)}B^{2(i-1)}}{p_k}\right)=0 \qquad (4.4)$$

ここで検討を分かり易くするために，$B^2=1$と仮定する．等式(4.4)は次のように書き換えられる．

$$\mathrm{Re}\left(\frac{C^2-1}{p_k}\right)\mathrm{Re}\left(\frac{\sum_{i=1}^{k}C^{2(k-i)}}{p_k}\right)=0 \qquad (4.4.1)$$

$$h=\mathrm{Re}\left(\frac{C^2}{p_k}\right)$$

$$h^2 = \mathrm{Re}\left(\frac{C^2}{p_k}\right)\ \mathrm{Re}\left(\frac{C^2}{p_k}\right) = \mathrm{Re}\left(\frac{C^{2*2}}{p_k}\right)$$

$$h^3 = \mathrm{Re}\left(\frac{C^2}{p_k}\right)\ \mathrm{Re}\left(\frac{C^2}{p_k}\right)\ \mathrm{Re}\left(\frac{C^2}{p_k}\right) = \mathrm{Re}\left(\frac{C^{2*3}}{p_k}\right)$$

…

$$h^i = \mathrm{Re}\left(\frac{C^2}{p_k}\right)\ \mathrm{Re}\left(\frac{C^2}{p_k}\right) \ldots\ \mathrm{Re}\left(\frac{C^2}{p_k}\right) = \mathrm{Re}\left(\frac{C^{2i}}{p_k}\right)$$

…

$$h^k = \mathrm{Re}\left(\frac{C^{2k}}{p_k}\right) = 1$$

$$\sum_{i=1}^{k} h^{k-i} = h^{k-1} + h^{k-2} + h^{k-3} + \cdots + h + 1$$

以上のように$h^i = \mathrm{Re}\left(\frac{C^{2(k-i)}}{p_k}\right)$ は位数kの巡回群の元である. $\sum_{i=1}^{k} h^{k-i}$は巡回群の元の総和である. その総和を素因数$p_k \neq 3$により剰余演算した剰余は以下に示すように0である.

等式(4.4.1)は次のように書き換えられる.

$$\mathrm{Re}\left(\frac{C^2-1}{p_k}\right)\mathrm{Re}\left(\frac{\sum_{i=1}^{k} C^{2(k-i)}}{p_k}\right) = \left(\mathrm{Re}\left(\frac{C^2}{p_k}\right) - \mathrm{Re}\left(\frac{1}{p_k}\right)\right)\left(\sum_{i=1}^{k}\mathrm{Re}\left(\frac{C^{2(k-i)}}{p_k}\right)\right) = 0$$

$$\left(\mathrm{Re}\left(\frac{C^2}{p_k}\right) - \mathrm{Re}\left(\frac{1}{p_k}\right)\right) = \mathrm{Re}\left(\frac{C^2}{p_k}\right) - 1 = h - 1 = 0 \qquad (4.4.1.1)$$

この等式(4.4.1.1)は素因数$p_k = 3$でのみ成立する.

$$\sum_{i=1}^{k}\mathrm{Re}\left(\frac{C^{2(k-i)}}{p_k}\right) = \mathrm{Re}\left(\frac{\sum_{i=1}^{k} h^{k-i}}{p_k}\right) = 0 \qquad (4.4.1.2)$$

この等式(4.4.1.2)は素因数$p_k \neq 3$でのみ成立する.

以上のことは$g = \mathrm{Re}\left(\frac{B^2}{p_k}\right)$にも当てはまる.

即ち, $g = \mathrm{Re}\left(\frac{B^2}{p_k}\right)$も$h$と同様に位数$k$の巡回群である.

等式(4.4.1.2)は次のように書き換えられる.

$$\sum_{i=1}^{k}\mathrm{Re}\left(\frac{C^{2(k-i)}B^{2(i-1)}}{p_k}\right) = \mathrm{Re}\left(\frac{\sum_{i=1}^{k} h^{(k-i)}g^{(i-1)}}{p_k}\right) = \sum_{i=1}^{k}\mathrm{Re}\left(\frac{h^{(k-i)}g^{(i-1)}}{p_k}\right) = 0$$

(4.4.1.3)

6. 補遺 2

$$\mathrm{Re}\left(\frac{C^{2km}-B^{2km}}{p_k}\right)=\mathrm{Re}\left(\frac{B^{2km}\left(\left(\frac{C^{2km}}{B^{2km}}\right)-1\right)}{p_k}\right)=\mathrm{Re}\left(\frac{B^{2km}}{p_k}\right)\mathrm{Re}\left(\frac{(C/B)^{2km}-1}{p_k}\right)=0$$

$$\mathrm{Re}\left(\frac{B^{2km}}{p_k}\right)=1$$

$$\mathrm{Re}\left(\frac{C^{2km}-B^{2km}}{p_k}\right)=\mathrm{Re}\left(\frac{(C/B)^{2km}-1}{p_k}\right)=\mathrm{Re}\left(\frac{(\frac{C}{B})^{2}-1}{p_k}\right)\mathrm{Re}\left(\frac{\sum_{i=1}^{k}(\frac{C}{B})^{2(k-i)}}{p_k}\right)=0$$

$$\mathrm{Re}\left(\frac{(\frac{C}{B})^{2}-1}{p_k}\right)=0 \qquad (6.1)$$

又は

$$\mathrm{Re}\left(\frac{\sum_{i=1}^{k}(\frac{C}{B})^{2(k-i)}}{p_k}\right)=0 \qquad (6.2)$$

等式(6.1)について検討する.

$$\mathrm{Re}\left(\frac{(\frac{C}{B})^{2}}{p_k}\right)=1$$

自然数Cと自然数Bは素因数を共有しないから，C/Bは有理数である.
有理数Zに対しても剰余演算が成立することが判る.

$C/B=Z$

$$\mathrm{Re}\left(\frac{Z^{2}-1}{p_k}\right)=0 \qquad (6.3)$$

$$\mathrm{Re}\left(\frac{\sum_{i=1}^{k}Z^{2(k-i)}}{p_k}\right)=0 \qquad (6.4)$$

Zが複素数の場合は剰余演算が成立するのであろうか？
有理数が複素数比で表せるのであれば可能であろう.