フェルマーの最終定理(ＦＬＴ)の証明

東森秀朋　2024.06.22

要約

指数が素数p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，因子$(2p+1)$が素数か否かに関わらず，その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，因子$(2p+1)$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，因子$(2p+1)$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因子$(2p+1)$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，ＦＬＴは証明される．

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．

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

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．

下記の中央の表記が正しいが，簡略して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.　因子$(2p+1)$による剰余はp個である

以下に，因子$(2p+1)$が素数であるか否かに関わらず，下記等式(2.1)の成立が証明される．

自然数A及びBは互いに素であり，いずれも因子$(2p+1)$を含まない．

$$\left(\frac{A^{2p}}{2p+1}\right) - \left(\frac{B^{2p}}{2p+1}\right) = \left(\frac{A^{2p}-B^{2p}}{2p+1}\right) = 0 \qquad (2.1)$$

次の等式(2.2)が成立する．

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

$$\left(\frac{\sum_{i=1}^{p}A^{2(p-i)}B^{2(i-1)}}{2p+1}\right)=\sum_{i=1}^{p}\left(\frac{A^{2(p-i)}B^{2(i-1)}}{2p+1}\right)=\sum_{i=1}^{p}\left(\frac{(A^{(p-i)}B^{(i-1)})^2}{2p+1}\right)\qquad(2.2)$$

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

上記から判るように，D^2の因子$(2p+1)$による剰余$\left(\frac{D^2}{2p+1}\right)$は$p$個である．

$$i=1\sim p$$

$$E:\quad 1\quad 2\quad 3\ldots\ldots\ p\quad p+1\ \ldots\ldots\ p+i\ \ldots\ldots\ 2p-1\quad 2p$$

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

$$E^2:1\quad 4\quad 9\ \ldots\ldots\ p^2\quad (p+1)^2\ \ldots\ (p+i)^2\ldots(2p-1)\ (2p)^2$$

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

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

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

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

以上のとおり，E^2の因子$(2p+1)$による剰余$\left(\frac{E^2}{2p+1}\right)$は以下に示す$p$個である．

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

そうすると，上記D^2のp個の剰余$\left(\frac{D^2}{2p+1}\right)$の各々は上記$E^2$の$p$個の剰余$\left(\frac{E^2}{2p+1}\right)$の何れかに必ず一致する．即ち，次の等式が成立する．

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

それ故，上記剰余(2.2)は以下の如く書き換えられ，等式(2.3)が成立する．

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

$$\sum_{i=1}^{p}\left(\frac{(A^{(p-i)}B^{(i-1)})^2}{2p+1}\right)=\sum_{j=1}^{p}\left(\frac{j^2}{2p+1}\right)=\left(\frac{\sum_{j=1}^{p}j^2}{2p+1}\right)=\left(\frac{p(p+1)(2p+1)/6}{2p+1}\right)\qquad(2.3)$$

$$\left(\frac{A^{2p}-B^{2p}}{2p+1}\right)=\left(\frac{A^2-B^2}{2p+1}\right)\sum_{i=1}^{p}\left(\frac{(A^{(p-i)}B^{(i-1)})^2}{2p+1}\right)=\left(\frac{A^2-B^2}{2p+1}\right)\left(\frac{p(p+1)(2p+1)/6}{2p+1}\right)\qquad(2.4)$$

3.　因子(2p+1)が素数でないときでも等式(2.1)は成立する

そこで，以下では，因子$(2p+1)$が素数であるか否かに関わらず，等式(2.1)は成立することが証明される．

3.1 あらゆる素数pはp_+又はp_-として表記される．

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，素数$(2k+1)$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，あらゆる素数p_kは次の２系列の数列のいずれかに含まれる．

mは自然数

$k = 3m$　　$p_+ = 6m+1$

$k+1 = 3m$　　$p_- = 6m-1$

そこで，上記２系列の数列に含まれる素数pを素数p_+または素数p_-と表記する．

3.2 $p = p_+$のとき等式(2.1)は成立する．

$$p_+ = 6m+1$$

$$2p_+ + 1 = 2(6m+1) + 1 = 12m + 3 = 3(4m+1)$$

因子$(2p_+ + 1)$で剰余演算したとき，p_iを含む二乗項は出現しない．

二乗項の総和からp_iを含む二乗項の和は差し引かれる．

p_iは素数である　　$p_{i-1} < p_i < p_{i+1}$　　i及びnは自然数である

$p_1 = 3$　　$2p_+ + 1 = {p_1}^{n_1}{p_2}^{n_2}{p_3}^{n_3} \ldots {p_i}^{n_i} \ldots . {p_n}^{n_n} = 3(4m+1)$

$l_i = ({p_1}^{n_1}{p_2}^{n_2}{p_3}^{n_3} \ldots {p_i}^{n_i-1} \ldots . {p_n}^{n_n} - 1)/2$

$2l_i + 1 = {p_1}^{n_1}{p_2}^{n_2}{p_3}^{n_3} \ldots {p_i}^{n_i-1} \ldots . {p_n}^{n_n}$

$$\begin{aligned}
{p_i}^2 + (2p_i)^2 + (3p_i)^2 + \cdots + (l_i p_i)^2 &= l_i(l_i+1)(2l_i+1){p_i}^2/6 \\
&= l_i(l_i+1)({p_1}^{n_1}{p_2}^{n_2}{p_3}^{n_3} \ldots {p_i}^{n_i-1} \ldots {p_n}^{n_n}){p_i}^2/6 \\
&= l_i(l_i+1)p_i({p_1}^{n_1}{p_2}^{n_2}{p_3}^{n_3} \ldots {p_i}^{n_i} \ldots {p_n}^{n_n})/6 \\
&= l_i(l_i+1)p_i(2p_+ + 1)/6 \\
&= l_i(l_i+1)p_i(3(4m+1))/6 \\
&= l_i(l_i+1)p_i(4m+1)/2
\end{aligned}$$

以下にp_iとp_jの重複を計算する．

$l_{ij} = ({p_1}^{n_1}{p_2}^{n_2}{p_3}^{n_3} \ldots {p_i}^{n_i-1} \ldots {p_j}^{n_j-1} \ldots . {p_n}^{n_n} - 1)/2$

$2l_{ij} + 1 = {p_1}^{n_1}{p_2}^{n_2}{p_3}^{n_3} \ldots {p_i}^{n_i-1} \ldots {p_j}^{n_j-1} \ldots . {p_n}^{n_n}$

$$(p_ip_j)^2+(2p_ip_j)^2+(3p_ip_j)^2+\cdots+\left(l_{ij}p_ip_j\right)^2=l_{ij}\left(l_{ij}+1\right)(2l_{ij}+1)\left(p_ip_j\right)^2/6$$

$$=l_{ij}\left(l_{ij}+1\right)\left({p_1}^{n_1}{p_2}^{n_2}{p_3}^{n_3}\ldots{p_i}^{n_i-1}\ldots{p_j}^{n_j-1}\ldots.{p_n}^{n_n}\right)\left(p_ip_j\right)^2/6$$

$$=l_{ij}\left(l_{ij}+1\right)p_ip_j({p_1}^{n_1}{p_2}^{n_2}{p_3}^{n_3}\ldots{p_i}^{n_i}\ldots{p_n}^{n_n})/6$$

$$=l_{ij}\left(l_{ij}+1\right)p_ip_j(2p_++1)/6$$

$$=l_{ij}\left(l_{ij}+1\right)p_ip_j(4m+1)/2$$

$(2p+1)$が合成数のとき，オイラーの定理によれば次の等式が成立する．

$\varphi(2p+1)$はオイラーのφ関数であり，以下ではφと略記する．

$$\left(\frac{A^{2\varphi}-1}{2p_++1}\right)=\left(\frac{A^2-1}{2p_++1}\right)\left(\frac{\sum_{i=1}^{\varphi}\left(A^2\right)^{i-1}}{2p_++1}\right)=0$$

合成数$(2p_++1)$で剰余演算したとき，合成数の因子p_iを含む二乗項は出現しない．

したがって，二乗項の総和$\sum_{j=1}^{p_+}j^2$からp_iを含む二乗項の和は差し引かれる．

よって，以下の等式が成立する．

$$\left(\frac{\sum_{j=1}^{p_+}j^2}{2p_++1}\right)=\left(\frac{p_+(p_++1)(2p_++1)/6}{2p_++1}\right)=\left(\frac{p_+(p_++1)(4m+1)/2}{3(4m+1)}\right)$$

$$\left(\frac{\sum_{i=1}^{\varphi}\left(A^2\right)^{i-1}}{2p_++1}\right)=\left(\frac{\sum_{j=1}^{p_+}j^2-\sum_{i=1}^{n}(l_i(l_i+1)p_i(2p_++1)/6)+\sum_{j=i+1}^{n}\left(\sum_{i=1}^{n-1}\left(l_{ij}\left(l_{ij}+1\right)p_ip_j(2p_++1)/6\right)\right)}{2p_++1}\right)$$

$$=\left(\frac{\sum_{j=1}^{p_+}j^2}{2p_++1}\right)-\left(\frac{\sum_{i=1}^{n}(l_i(l_i+1)p_i(2p_++1)/6)}{(2p_++1)}\right)+\left(\frac{\sum_{j=i+1}^{n}\left(\sum_{i=1}^{n-1}\left(l_{ij}\left(l_{ij}+1\right)p_ip_j(2p_++1)/6\right)\right)}{(2p_++1)}\right)$$

$$=\left(\frac{p_+(p_++1)(4m+1)/2}{3(4m+1)}\right)-\left(\frac{\sum_{i=1}^{n}(l_i(l_i+1)p_i(4m+1)/2)}{3(4m+1)}\right)+\left(\frac{\sum_{j=i+1}^{n}\left(\sum_{i=1}^{n-1}\left(l_{ij}\left(l_{ij}+1\right)p_ip_j(4m+1)/2\right)\right)}{3(4m+1)}\right)$$

$$=\left(\left(\frac{p_+(p_++1)/2}{3(4m+1)}\right)-\left(\frac{\sum_{i=1}^{n}l_i(l_i+1)p_i/2}{3(4m+1)}\right)-\left(\frac{\sum_{j=i+1}^{n}\left(\sum_{i=1}^{n-1}\left(l_{ij}\left(l_{ij}+1\right)p_ip_j/2\right)\right)}{3(4m+1)}\right)\right)\left(\frac{4m+1}{3(4m+1)}\right)$$

$$Q=\left(\frac{\sum_{i=1}^{n}(l_i(l_i+1)p_i/2)}{3(4m+1)}\right)-\left(\frac{\sum_{j=i+1}^{n}\left(\sum_{i=1}^{n-1}\left(l_{ij}\left(l_{ij}+1\right)p_ip_j/2\right)\right)}{3(4m+1)}\right)$$

$$\left(\frac{\sum_{i=1}^{\varphi}\left(A^2\right)^{i-1}}{2p_++1}\right)=\left(\left(\frac{p_+(p_++1)/2}{3(4m+1)}\right)-Q\right)\left(\frac{4m+1}{3(4m+1)}\right)$$

$$\left(\frac{A^{2\varphi}-1}{2p+1}\right)=\left(\frac{A^2-1}{2p+1}\right)\left(\frac{\sum_{i=1}^{\varphi}\left(A^2\right)^{i-1}}{2p+1}\right)=\left(\frac{A^2-1}{2p_++1}\right)\left(\left(\frac{p_+(p_++1)/2}{3(4m+1)}\right)-Q\right)\left(\frac{4m+1}{3(4m+1)}\right)$$

$$=\left(\frac{A^2-1}{2p_++1}\right)\left(\frac{4m+1}{3(4m+1)}\right)\left(\left(\frac{p_+(p_++1)/2}{3(4m+1)}\right)-Q\right)$$

$$\left(\frac{A^2-1}{2p_++1}\right)\left(\frac{4m+1}{3(4m+1)}\right)=\left(\frac{\left(A^2-1\right)(4m+1)}{3(4m+1)}\right)=0$$

$$=0$$

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

以上のとおり，オイラーの定理が証明された.

そこで，$p=p_+$のとき等式(2.1)が成立することを証明する.

$$\left(\frac{A^{2p_+-1}}{2p_++1}\right)=\left(\frac{A^2-1}{2p_++1}\right)\left(\frac{\sum_{i=1}^{p_+}(A^2)^{i-1}}{2p_++1}\right)=\left(\frac{A^2-1}{2p_++1}\right)\left(\frac{\sum_{j=1}^{p_+}j^2}{2p_++1}\right)$$

$$=\left(\frac{A^2-1}{2p_++1}\right)\left(\frac{p_+(p_++1)(4m+1)/2}{3(4m+1)}\right)$$

$$=\left(\frac{A^2-1}{2p_++1}\right)\left(\frac{p_+(p_++1)/2}{3(4m+1)}\right)\left(\frac{4m+1}{3(4m+1)}\right)$$

$$=\left(\frac{A^2-1}{2p_++1}\right)\left(\frac{4m+1}{3(4m+1)}\right)\left(\frac{p_+(p_++1)/2}{3(4m+1)}\right)$$

$$\left(\frac{A^2-1}{2p_++1}\right)\left(\frac{4m+1}{3(4m+1)}\right)=\left(\frac{(A^2-1)(4m+1)}{3(4m+1)}\right)=0$$

$$=0$$

同様に次の等式が成立する.

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

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

以上のとおり，$p=p_+$のとき等式(2.1)は成立する

以下に例示される.

$p_+=19$　$(2p_++1)=39=3\times13$　$p_1=3$　$p_2=13$　$n=2$

$A=2$　$B=1$　$p_+=19$　$2p_++1=39$

そのとき，等式(2.3)は次のようになる.

$$\sum_{i=1}^{\varphi}\left(\frac{A^{2(\varphi-i)}}{2p_++1}\right)$$

$$=\left(\frac{\sum_{i=1}^{p_+}2^{2(p_+-i)}}{2p_++1}\right)-\left(\frac{\sum_{i=1}^{n}l_i(l_i+1)p_i(2p_++1)}{6(2p_++1)}\right)+\left(\frac{\sum_{j=i+1}^{n}(\sum_{i=1}^{n-1}l_{ij}(l_{ij}+1)p_ip_j/2)}{3(4m+1)}\right)$$

$$=\left(\frac{\sum_{j=1}^{19}j^2}{2p_++1}\right)-\left(\frac{3^2+6^2+9^2+12^2+15^2+18^2+13^2}{39}\right)$$

$$=\left(\frac{1+2^2+4^2+8^2+16^2+7^2+14^2+11^2+17^2+5^2+10^2+19^2}{39}\right)$$

$$=\left(\frac{1+2^2+(2^2)^2+(2^2)^3+(2^2)^4+(2^2)^5+(2^2)^6+(2^2)^7+(2^2)^8+(2^2)^9+(2^2)^{10}+(2^2)^{11}}{39}\right)$$

$$2^2=2^2$$

$(2^2)^2 = 4^2$
$(2^2)^3 = 8^2$
$(2^2)^4 = 16^2$
$(2^2)^5 = 7^2 + 39 \times 25$
$(2^2)^6 = 14^2 + 39 \times 100$
$(2^2)^7 = 11^2 + 39 \times 1673$
$(2^2)^8 = 17^2 + 39 \times 1673$
$(2^2)^9 = 5^2 + 39 \times 6721$
$(2^2)^{10} = 10^2 + 39 \times 26834$
$(2^2)^{11} = 19^2 + 39 \times 107{,}537$
$(2^2)^{12} = 1^2 + 39 \times 430{,}185$

$A = 7 \quad B = 1 \quad p_+ = 19 \quad 2p_+ + 1 = 39 = 3 \times 13$
$p_1 = 3 \quad p_2 = 13 \quad n = 2$
$7^2 = 7^2$
$(7^2)^2 = 10^2$
$(7^2)^3 = 8^2$
$(7^2)^4 = 17^2$
$(7^2)^5 = 2^2 + 39 \times 7{,}242{,}955$
$(7^2)^6 = 14^2 + 39 \times 354{,}904{,}795$
$(7^2)^7 = 19^2 + 39 \times 17{,}390{,}335{,}192$
$(7^2)^8 = 16^2 + 39 \times 852{,}126{,}424{,}855$
$(7^2)^9 = 5^2 + 39 \times 41{,}754{,}194{,}818{,}216$
$(7^2)^{10} = 4^2 + 39 \times 2{,}045{,}955{,}546{,}092{,}615$
$(7^2)^{11} = 11^2 + 39 \times 100{,}251{,}821{,}758{,}538{,}152$
$(7^2)^{12} = 1^2 + 39 \times 4{,}912{,}339{,}266{,}168{,}369{,}600$

$p_+ = 37 \quad (2p_+ + 1) = 75 = 3 \times 5^2 \quad p_1 = 3 \quad p_2 = 5 \quad n = 2$
$A = 2 \quad B = 1 \quad p_+ = 37 \quad 2p_+ + 1 = 75$
そのとき，等式(2.3)は次のようになる．

$$\sum_{i=1}^{\varphi}\left(\frac{A^{2(\varphi-i)}}{2p_+ +1}\right)$$

$$= \left(\frac{\sum_{i=1}^{p_+} 2^{2(p_+-i)}}{2p_+ +1}\right) - \left(\frac{\sum_{i=1}^{n} l_i(l_i+1)p_i(2p_+ +1)/2}{2p_+ +1}\right) + \left(\frac{\sum_{j=i+1}^{n}\left(\sum_{i=1}^{n-1} l_{ij}(l_{ij}+1)p_i p_j/2\right)}{2p_+ +1}\right)$$

$$= \left(\frac{\sum_{i=1}^{37} i^2}{75}\right) - \left(\frac{3^2+6^2+9^2+12^2+15^2+18^2+21^2+24^2+27^2+30^2+33^2+36^2}{75}\right)$$

$$-\left(\frac{5^2+10^2+15^2+20^2+25^2+30^2+35^2}{75}\right)$$

$$+\left(\frac{15^2+30^2}{75}\right)$$

$$=\left(\frac{1+2^2+4^2+8^2+16^2+32^2+11^2+\cdots+7^2+14^2+28^2+19^2+37^2}{75}\right)$$

$$=\left(\frac{1+2^2+(2^2)^2+(2^2)^3+\cdots+(2^2)^{19}}{75}\right)$$

$$2^2 = 2^2$$
$$(2^2)^2 = 4^2$$
$$(2^2)^3 = 8^2$$
$$(2^2)^4 = 16^2$$
$$(2^2)^5 = 32^2$$
$$(2^2)^6 = 11^2 + 75 \times 53$$
$$(2^2)^7 = 22^2$$
$$(2^2)^8 = 31^2 + 75 \times 861$$
$$(2^2)^9 = 13^2 + 75 \times 3493$$
$$(2^2)^{10} = 26^2 + 75 \times 13{,}972$$
$$(2^2)^{11} = 23^2 + 75 \times 55{,}917$$
$$(2^2)^{12} = 29^2 + 75 \times 223{,}685$$
$$(2^2)^{13} = 17^2 + 75 \times 894{,}781$$
$$(2^2)^{14} = 34^2 + 75 \times 3{,}579{,}124$$
$$(2^2)^{15} = 7^2 + 75 \times 14{,}316{,}557$$
$$(2^2)^{16} = 14^2 + 75 \times 57{,}266{,}228$$
$$(2^2)^{17} = 28^2 + 75 \times 229{,}064{,}912$$
$$(2^2)^{18} = 19^2 + 75 \times 916{,}259{,}685$$
$$(2^2)^{19} = 37^2 + 75 \times 3{,}665{,}038{,}741$$
$$(2^2)^{20} = 1^2 + 75 \times 14{,}660{,}155{,}037$$

3.3 $p = p_-$のとき等式(2.1)は成立する.

3.3.1 $p = p_-$のとき，因子$(2p_- + 1)$が素数であるならば，下記等式(2.1)は成立する.

$$p_- = 6m - 1 \qquad 2p_- + 1 = 12m - 1$$

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

$$\left(\frac{A^{2p_-}-B^{2p_-}}{2p_-+1}\right)=\left(\frac{A^{2p_-}}{2p_-+1}\right)-\left(\frac{B^{2p_-}}{2p_-+1}\right)=0 \qquad (2.1)$$

$$A=2 \qquad B=1 \qquad p=11 \qquad 2p+1=23$$

$$\left(\frac{\sum_{i=1}^{p_-}A^{2(p-i)}B^{2(i-1)}}{2p_-+1}\right)=\left(\frac{1+4+4^2+4^3+4^4+4^5+4^6+4^7+4^8+4^9+4^{10}}{23}\right) =$$

$$\left(\frac{1+2^2+4^2+8^2+7^2+9^2+5^2+10^2+3^2+6^2+11^2}{23}\right)=\left(\frac{\sum_{j=1}^{11}j^2}{2p+1}\right)$$

$$4=2^2$$
$$4^2=16=4^2$$
$$4^3=64=8^2$$
$$4^4=256=7^2+23\times 11$$
$$4^5=1024=9^2+23\times 41$$
$$4^6=4096=5^2+23\times 177$$
$$4^7=16{,}384=10^2+23\times 708$$
$$4^8=65{,}536=3^2+23\times 2{,}849$$
$$4^9=262{,}144=6^2+23\times 11{,}396$$
$$4^{10}=1{,}048{,}576=11^2+23\times 45{,}585$$
$$4^{11}=4{,}194{,}304=1^2+23\times 182{,}361$$

3.3.2 因子$(2p_-+1)$が素数でないときでも，下記の如く等式(2.1)は成立する．

因子$(2p_-+1)$で剰余演算したとき，p_iを含む二乗項は出現しない．

二乗項の総和$\sum_{j=1}^{p_-}j^2$からp_iを含む二乗項の和は差し引かれる．

$p_i\geq 5$は素数である　　$p_{i-1}<p_i<p_{i+1}$　　$i=1\sim n$

$$2p_-+1={p_1}^{n_1}{p_2}^{n_2}{p_3}^{n_3}\ldots{p_i}^{n_i}\ldots.{p_n}^{n_n}$$
$$l_i=({p_1}^{n_1}{p_2}^{n_2}{p_3}^{n_3}\ldots{p_i}^{n_i}\ldots.{p_n}^{n_n}-1)/2$$
$$2l_i+1={p_1}^{n_1}{p_2}^{n_2}{p_3}^{n_3}\ldots{p_i}^{n_i}\ldots.{p_n}^{n_n}$$
$$\begin{aligned}{p_i}^2+(2p_i)^2+(3p_i)^2\ldots+(l_ip_i)^2&=l_i(l_i+1)(2l_i+1){p_i}^2/6\\&=l_i(l_i+1)({p_1}^{n_1}{p_2}^{n_2}{p_3}^{n_3}\ldots{p_i}^{n_i-1}\ldots.{p_n}^{n_n}){p_i}^2/6\\&=l_i(l_i+1)({p_1}^{n_1}{p_2}^{n_2}{p_3}^{n_3}\ldots{p_i}^{n_i}\ldots.{p_n}^{n_n})p_i/6\\&=l_i(l_i+1)p_i(2p_-+1)/6\end{aligned}$$

$p_i\geq 5$であるから$l_i(l_i+1)$は数6の倍数である．

以下にp_iとp_jの重複が計算される．

$$l_{ij}=({p_1}^{n_1}{p_2}^{n_2}{p_3}^{n_3}\ldots{p_i}^{n_i-1}\ldots{p_j}^{n_j-1}\ldots.{p_n}^{n_n}-1)/2$$
$$2l_{ij}+1={p_1}^{n_1}{p_2}^{n_2}{p_3}^{n_3}\ldots{p_i}^{n_i-1}\ldots{p_j}^{n_j-1}\ldots.{p_n}^{n_n}$$

$$(p_ip_j)^2+(2p_ip_j)^2+(3p_ip_j)^2+\cdots+\left(l_{ij}p_ip_j\right)^2=l_{ij}\left(l_{ij}+1\right)(2l_{ij}+1)\left(p_ip_j\right)^2/6$$

$$= l_{ij}\left(l_{ij}+1\right)\left({p_1}^{n_1}{p_2}^{n_2}{p_3}^{n_3}\ldots{p_i}^{n_i-1}\ldots{p_j}^{n_j-1}\ldots.{p_n}^{n_n}\right)\left(p_ip_j\right)^2/6$$

$$= l_{ij}\left(l_{ij}+1\right)p_ip_j({p_1}^{n_1}{p_2}^{n_2}{p_3}^{n_3}\ldots{p_i}^{n_i}\ldots{p_n}^{n_n})/6$$

$$= l_{ij}\left(l_{ij}+1\right)p_ip_j(2p_-+1)/6$$

$$= l_{ij}\left(l_{ij}+1\right)p_ip_j(12m-1)/6$$

等式(2.3)は次の如く書き換えられる.

$$\left(\frac{\sum_{j=1}^{\varphi}A^{2(i-1)}}{2p_-+1}\right)=\left(\frac{\sum_{j=1}^{p_-}j^2-\sum_{i=1}^{n}(l_i(l_i+1)p_i(2p_-+1)/6)+\sum_{j=i+1}^{n}(\sum_{i=1}^{n-1}(l_{ij}(l_{ij}+1)p_ip_j(2p_-+1)/6))}{2p_-+1}\right)$$

$$=\left(\frac{\sum_{j=1}^{p_-}j^2}{2p_-+1}\right)-\left(\frac{\sum_{i=1}^{n}(l_i(l_i+1)p_i(2p_-+1))/6)}{(2p_-+1)}\right)+\left(\frac{\sum_{j=i+1}^{n}(\sum_{i=1}^{n-1}(l_{ij}(l_{ij}+1)p_ip_j(2p_-+1)/6))}{(2p_-+1)}\right)$$

$$=\left(\frac{p_-(p_-+1)(12m-1)/6}{12m-1}\right)-\left(\frac{\sum_{i=1}^{n}(l_i(l_i+1)p_i(12m-1)/6)}{12m-1}\right)$$

$$+\left(\frac{\sum_{j=i+1}^{n}(\sum_{i=1}^{n-1}(l_{ij}(l_{ij}+1)p_ip_j(12m-1)/6))}{12m-1}\right)$$

$$=\left(\left(\frac{p_-(p_-+1)/6}{12m-1}\right)-\left(\frac{\sum_{i=1}^{n}(l_i(l_i+1)p_i/6)}{12m-1}\right)+\left(\frac{\sum_{j=i+1}^{n}(\sum_{i=1}^{n-1}(l_{ij}(l_{ij}+1)p_ip_j/6))}{12m-1}\right)\right)\left(\frac{12m-1}{12m-1}\right)$$

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

$$=0$$

$$\left(\frac{A^{2\varphi}-1}{2p_-+1}\right)=\left(\frac{A^2-1}{2p_-+1}\right)\left(\frac{\sum_{j=1}^{\varphi}A^{2(i-1)}}{2p_-+1}\right)=0$$

因子$(2p_-+1)$が合成数ときでも，下記の如く等式(2.1)は成立する.

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

$$=\left(\frac{A^2-B^2}{2p_-+1}\right)\left(\frac{p_-(p_-+1)(12m-1)/6}{12m-1}\right)$$

$$=\left(\frac{A^2-B^2}{2p_-+1}\right)\left(\frac{p_-(p_-+1)/6}{12m-1}\right)\left(\frac{12m-1}{12m-1}\right)$$

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

$$=0$$

因子$(2p_-+1)$が素数でない例を以下に示す.

$p_-=17$　　$(2p_-+1)=35=5\times7$　　$p_1=5$　　$p_2=7$　　$n=2$

$A=2$　　$B=1$

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

$$= \left(\frac{\sum_{j=1}^{17} j^2}{35}\right) - \left(\frac{5^2+10^2+15^2+7^2+14^2}{35}\right)$$

$$= \left(\frac{1+2^2+4^2+8^2+16^2+3^2+6^2+12^2+11^2+13^2+9^2+17^2}{35}\right)$$

$$= \left(\frac{1+2^2+(2^2)^2+(2^2)^3+(2^2)^4+(2^2)^5+(2^2)^6+(2^2)^7+(2^2)^8+(2^2)^9+(2^2)^{10}+(2^2)^{11}}{35}\right)$$

$2^2 = 2^2$

$(2^2)^2 = 4^2$

$(2^2)^3 = 8^2$

$(2^2)^4 = 16^2$

$(2^2)^5 = 3^2 + 35 \times 29$

$(2^2)^6 = 6^2 + 35 \times 116$

$(2^2)^7 = 12^2 + 35 \times 464$

$(2^2)^8 = 11^2 + 35 \times 1869$

$(2^2)^9 = 13^2 + 35 \times 7485$

$(2^2)^{10} = 9^2 + 35 \times 29957$

$(2^2)^{11} = 17^2 + 35 \times 119829$

$(2^2)^{12} = 1^2 + 35 \times 479349$

$A = 3 \qquad B = 1 \qquad p_- = 17 \qquad 2p_- + 1 = 35$

$3^2 = 3^2$

$(3^2)^2 = 9^2$

$(3^2)^3 = 8^2 + 35 \times 19$

$(3^2)^4 = 11^2 + 35 \times 184$

$(3^2)^5 = 2^2 + 35 \times 1687$

$(3^2)^6 = 6^2 + 35 \times 116$

$(3^2)^7 = 17^2 + 35 \times 15183$

$(3^2)^8 = 16^2 + 35 \times 1869$

$(3^2)^9 = 13^2 + 35 \times 11{,}069{,}152$

$(3^2)^{10} = 4^2 + 35 \times 99{,}622{,}411$

$(3^2)^{11} = 12^2 + 35 \times 896{,}601{,}699$

$(3^2)^{12} = 1^2 + 35 \times 8{,}069{,}415{,}328$

以上のとおり，因子$(2p+1)$が素数であるか否かに関わらず，等式(2.1)は成立する．

4. 因子$(2p+1)$による剰余演算においてフェルマーの等式は成立しない.

下記等式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.

自然数A及びBのいずれも因子$(2p+1)$を含まない.

$$U = A^p - B^p \qquad\qquad V = A^p + B^p$$

上記等式(2.1)は次のように変形される.

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

因子$(2p+1)$が素数である場合には自然数U又はVは因子$(2p+1)$を含む.

自然数Uが因子$(2p+1)$を含むとき，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.

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

しかしながら，上記等式が成立しないことを以下に示す.

等式(2.1)において$A = 1$又は$B = 1$とすると，次の等式が得られる.

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

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

以上のとおり, 因子$(2p+1)$による剰余演算においてフェルマーの等式(1.1)は成立しない.

したがって，フェルマーの等式(1.1)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

因子$(2p+1)$が素数でない場合，例えば，素数p_1と素数p_2の積$p_1p_2 = (2p+1)$である場合，には次のことが考えられる.

自然数Uが素数p_1を含みそして自然数Vが素数p_2を含む場合或いはその逆の場合が考えられる.

$$\left(\frac{A^{2p}-B^{2p}}{2p+1}\right) = \left(\frac{A^p-B^p}{2p+1}\right)\left(\frac{A^p+B^p}{2p+1}\right) = \left(\frac{U}{2p+1}\right)\left(\frac{V}{2p+1}\right) = \left(\frac{UV}{p_1p_2}\right) = 0$$

以上の場合はあり得ないことを以下に証明する.

素数p_1は自然数U又はVの何れかに含まれるから，自然数A及びBの如何に関わらず次の等式が成立しなければならない.

$$\left(\frac{UV}{p_1}\right) = 0$$

しかしながら，以下に示すように自然数A及びBの如何に関わらずに上記等式が成立することはない.

$$\left(\frac{UV}{p_1}\right) = \left(\frac{A^{p_1p_2-1} - B^{p_1p_2-1}}{p_1}\right) = \left(\frac{A^{p_1p_2-1}}{p_1}\right) - \left(\frac{B^{p_1p_2-1}}{p_1}\right)$$

$$= \left(\frac{A^{p_2(p_1-1)+p_2-1}}{p_1}\right) - \left(\frac{B^{p_2(p_1-1)+p_2-1}}{p_1}\right)$$

$$= \left(\frac{A^{p_2(p_1-1)}}{p_1}\right)\left(\frac{A^{p_2-1}}{p_1}\right) - \left(\frac{B^{p_2(p_1-1)}}{p_1}\right)\left(\frac{B^{p_2-1}}{p_1}\right)$$

$$\left(\frac{A^{p_2(p_1-1)}}{p_1}\right) = \left(\frac{B^{p_2(p_1-1)}}{p_1}\right) = \left(\frac{1}{p_1}\right)$$

$$= \left(\frac{A^{p_2-1}}{p_1}\right) - \left(\frac{B^{p_2-1}}{p_1}\right) \neq 0$$

つまり，積$p_1p_2 = (2p+1)$は自然数U又はVの何れかに含まれねばならない.

以上のことは次の場合においても成立することは数学的帰納法により証明される．ここではその証明は省略される.

$$p_1p_2p_3 \cdots p_n = (2p+1)$$

よって，自然数A及びBのいずれも因子$(2p+1)$を含まないとき，その因子$(2p+1)$が素数であるか否かに関わらずに，FLT は証明された.

また，自然数B及びCのいずれも因子$(2p+1)$を含まないときも，上記と同様にして FLT は証明される.

以上のとおり， FLT は証明された.

３． 結論

指数が素数pのフェルマーの等式は因子$(2p+1)$による剰余演算において成立しないから，そ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.

４． 参考文献

[1] Adleman LM, Heath-Brown DR (June 1985). "The first case of Fermat's last theorem". Inventiones Mathematicae. Berlin: Springer. 79 (2): 409–416. Bibcode:1985InMat..79..409A.

doi:10.1007/BF01388981. S2CID 122537472.
[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.