The idea of the Arithmetica

Hajime Mashima

April 27, 2014

Abstract

During the 360 years of Fermat's last theorem is to be proved, this proposition was the presence appear full-length novel in "The Lord of the Rings", such as the "One Ring". And finally in 1994, it was proved completely by Andrew Wiles. However interesting proof is Fermat has been is still unknown. This will be assumed in the category of algebra probably.

introduction

Natural number X,Y and Z solution of 3 or more that this equation holds $X^n + Y^n = Z^n$ does not exist. Fermat is proven for the conditions of n = 4. It is sufficient if n is examining the conditions of prime numbers greater than or equal to 3 for this.

Theorem 1 *Triangle the hypotenuse of Pythagorean theorem is z, can be expressed by the following relation by using the l and m.*

$$\left(l^2 - m^2\right)^2 + 2^2 \left(lm\right)^2 = \left(l^2 + m^2\right)^2$$

$$\begin{aligned} x^2 &= \left(l^2 - m^2\right)^2 \\ y^2 &= 2^2 \left(lm\right)^2 \\ z^2 &= \left(l^2 + m^2\right)^2 \end{aligned}$$

$(xyz \neq 0)$

To simplify the algebra as a real number M, and N.

$M, N \in \mathbb{R} \qquad l^2 = M, \ m^2 = N$

$$\left(M - N\right)^2 + 2^2 MN = \left(M + N\right)^2$$

Put $\quad X,Y,Z \in \mathbb{N}\ number \qquad prime\ number = p \geq 3$

$$\begin{aligned} X^p &= (M-N)^2 \\ Y^p &= 2^2 MN \\ Z^p &= (M+N)^2 \end{aligned}$$

$(XYZ \neq 0)$

Add the following conditions. $\quad X,Y,Z \in even\ number$

$$\begin{aligned} X^p &= 2^p X_1^p \\ Y^p &= 2^p Y_1^p \\ Z^p &= 2^p Z_1^p \end{aligned}$$

$(X_1, Y_1, Z_1 \in \mathbb{N})$

$MN = 2^{p-2} Y_1^p \in \mathbb{N}$

Thus M, N is a rational or irrational both.

1 M,N is a condition of both rational

$X^p = 2^p X_1^p \ , \ Z^p = 2^p Z_1^p$
$M-N, M+N \in even number$, and it will be a divisor of $2^{\frac{p+1}{2}}$ at least.

Consequently, $Y_1^p \in even\ number$ so $X_1^p \ , \ Z_1^p \in even\ number.$ (1)

2 M,N is a condition of both irrational

$$\begin{aligned} MN &= 2^{p-2} Y_1^p \\ &= 2^{p-2} \left(Z_1^p - X_1^p\right) \\ &= 2^{p-2} \left(\sqrt{Z_1^p} + \sqrt{X_1^p}\right)\left(\sqrt{Z_1^p} - \sqrt{X_1^p}\right) \end{aligned}$$

$X^p = 2^p X_1^p \ , \ Z^p = 2^p Z_1^p$

$$M = \left(\sqrt{2^{p-2} Z_1^p} + \sqrt{2^{p-2} X_1^p}\right) \quad N = \left(\sqrt{2^{p-2} Z_1^p} - \sqrt{2^{p-2} X_1^p}\right) \quad (M > N)$$

Put$(c, d \in odd\ number \qquad l, m \in \mathbb{N})$
$M = 2^{\frac{l}{2}} c^{\frac{1}{2}} + 2^{\frac{m}{2}} d^{\frac{1}{2}} \qquad N = 2^{\frac{l}{2}} c^{\frac{1}{2}} - 2^{\frac{m}{2}} d^{\frac{1}{2}} \qquad$ (I)

In addition, assuming that there is no difference and sum,

Put$(U, V \in odd\ \ number)$
$M = 2^{\frac{l}{2}}U \qquad\qquad N = 2^{\frac{m}{2}}V \qquad\qquad (\mathrm{II})$

$MN = 2^{p-2}Y_1^p = 2^{\frac{l+m}{2}}UV \in \mathbb{N}$
M, N because irrational both,therefore$(l, m \in odd\ \ number)$.

2.1 Conditions of (II)

2.1.1 Conditions of $(Y_1^p \in odd\ \ number)$

$Y_1^p = Z_1^p - X_1^p$

Z_1^p, X_1^p is the relationship of "odd and even" or "odd and even".

Z_1^p and X_1^p are assumed to be coprime.Common divisor $R^p\,(\in odd\ \ number)$, if present in the Z_1^p and X_1^p , is included as a common divisor of R^p also Y_1^p. $(\frac{Y_1^p}{R^p} \in \mathbb{N})$
It is possible to remove common divisor, it is sufficient Z_1^p and X_1^p is examining the conditions of coprime.

$MN = 2^{p-2}Y_1^p = 2^{\frac{l+m}{2}}UV \qquad (p = \frac{l+m}{2} + 2 \qquad Y_1^p = UV)$

Proposition 2 $l > m \qquad \frac{l+m}{2} > m\ (l, m \in odd\ \ number \quad U, V \in odd\ \ number)$

$\underline{odd\ \ number = 2^{\frac{l-m}{2}+2}X_1^p}$

$$\begin{aligned} X^p &= (M-N)^2 \\ &= M^2 + N^2 - 2MN \\ &= 2^l U^2 + 2^m V^2 - 2 \cdot 2^{\frac{l+m}{2}}UV \\ &= 2^m \left(2^{l-m}U^2 + V^2 - 2 \cdot 2^{\frac{l-m}{2}}UV\right) \\ &= 2^m\,(odd\ \ number) \end{aligned}$$

$$X^p = 2^m \left(2^{\frac{l-m}{2}+2}X_1^p\right)$$

$$odd\ \ number \neq 2^{\frac{l-m}{2}+2}X_1^p \qquad (2)$$

Lemma 3 $l = p-2 \qquad m = p-2\ (l, m \in odd\ \ number \quad U, V \in odd\ \ number)$

Other things being does not hold all applies the infinite descent.

$$X^p = (M-N)^2 = \left(2^{\frac{p-2}{2}}U - 2^{\frac{p-2}{2}}V\right)^2 = 2^{p-2}(U-V)^2$$

$$\begin{aligned} 2^2 X_1^p &= (U-V)^2 \qquad (U>V) \\ 2\sqrt{X_1^p} &= U-V \qquad \cdots① \end{aligned}$$

$$Z^p = (M+N)^2 = \left(2^{\frac{p-2}{2}}U + 2^{\frac{p-2}{2}}V\right)^2 = 2^{p-2}(U+V)^2$$

$$\begin{aligned} 2^2 Z_1^p &= (U+V)^2 \qquad (U>V) \\ 2\sqrt{Z_1^p} &= U+V \qquad \cdots② \end{aligned}$$

X_1^p, Z_1^p is a square number $U \pm V$ because it is a natural number.

$X_1^p = (X_{II}^p)^2 \quad Z_1^p = (Z_{II}^p)^2 \quad (X_{II}^p, Z_{II}^p \in \mathbb{N})$

simultaneous equation:①±②

$$U = Z_{II}^p + X_{II}^p \qquad V = Z_{II}^p - X_{II}^p$$

If U,V is not a coprime, and a common divisor r($\in$ *odd number*).

$$\begin{aligned} U &= Z_{II}^p + X_{II}^p = rf \qquad \cdots③ \\ V &= Z_{II}^p - X_{II}^p = rg \qquad \cdots④ \end{aligned}$$

$(U, V \in \textit{odd number} \qquad f, g \in \textit{odd number})$

simultaneous equation:③±④

$$\begin{aligned} 2Z_{II}^p &= r(f+g) \\ 2X_{II}^p &= r(f-g) \end{aligned}$$

X_{II}^p, Z_{II}^p comprises a common divisor r. butX_{II}^p, Z_{II}^pmust also be coprime X_1^p, Z_1^p is coprime. Thus U, V is coprime.

Theorem 4 $(Y_1^p = UV)$ *U, V is at a coprime, which is a power of a prime number.*

$$U = U_{II}^p \ , \ V = V_{II}^p \qquad Y_1^p = (U_{II}V_{II})^p$$

Substitute U_{II}^p, V_{II}^p for ③,④.

$$U_{II}^p = Z_{II}^p + X_{II}^p \qquad V_{II}^p + X_{II}^p = Z_{II}^p \tag{3}$$

2.1.2 Conditions of ($Y_1^p \in even\ \ number$)

$(Y^p = 2^2 MN)$ MN because it has a divisor in 2^{2p-2} at least,

$$\frac{l+m}{2} \geq 2p-2 \qquad M = 2^{\frac{l}{2}} U \ , \ N = 2^{\frac{m}{2}} V \quad (U, V \in odd\ \ number)$$

Proposition 5 $p > m$ $(l+m \geq 2(2p-2)$ $l > m$ $l, m \in odd\ \ number)$

$\underline{odd\ \ number = 2^{p-m} X_1^p}$

$$\begin{aligned} X^p &= (M-N)^2 \\ &= M^2 + N^2 - 2MN \\ &= 2^l U^2 + 2^m V^2 - 2 \cdot 2^{\frac{l+m}{2}} UV \\ &= 2^m \left(2^{l-m} U^2 + V^2 - 2 \cdot 2^{\frac{l-m}{2}} UV \right) \\ &= 2^m \, (odd\ \ number) \end{aligned}$$

$$X^p = 2^p X_1^p = 2^m \left(2^{p-m} X_1^p \right)$$

$$odd\ \ number \neq 2^{p-m} X_1^p \tag{4}$$

Proposition 6 $p = m$ $(l+m \geq 2(2p-2)$ $l > m$ $l, m \in odd\ \ number)$

$\underline{V \in even\ \ number}$

$$\begin{aligned} l + p &\geq 2(2p-2) \\ l &\geq 2(2p-2) - p \end{aligned}$$

$(l, p \in odd\ \ number \qquad q \in even\ \ number)$

$$\begin{aligned} l &= 2(2p-2) - p + q \\ l &= 4(p-1) - p + q \end{aligned}$$

$$\begin{aligned} X^p &= (M-N)^2 \\ &= M^2 + N^2 - 2MN \\ &= 2^l U^2 + 2^m V^2 - 2 \cdot 2^{\frac{l+m}{2}} UV \\ &= 2^{4(p-1)-p+q} U^2 + 2^p V^2 - 2 \cdot 2^{2(p-1)+\frac{q}{2}} UV \\ &= 2^p \left(2^{4(p-1)-2p+q} U^2 + V^2 - 2 \cdot 2^{2(p-1)-p+\frac{q}{2}} UV \right) \\ &= 2^p \left(\left(2^{2(p-1)-p+\frac{q}{2}} U \right)^2 + V^2 - 2 \cdot 2^{2(p-1)-p+\frac{q}{2}} UV \right) \\ &= 2^p \left(2^{p-2+\frac{q}{2}} U - V \right)^2 \\ &= 2^p X_1^p \\ X_1^p &= \left(2^{p-2+\frac{q}{2}} U - V \right)^2 \end{aligned}$$

Similarly,

$$\begin{aligned} Z^p &= 2^p \left(2^{p-2+\frac{q}{2}}U + V\right)^2 \\ &= 2^p Z_1^p \\ Z_1^p &= \left(2^{p-2+\frac{q}{2}}U + V\right)^2 \end{aligned}$$

X_1^p, Z_1^p is a square number $2^{p-2+\frac{q}{2}}U + V$ because it is a natural number.

$X_1^p = (X_{II}^p)^2 \ , \ Z_1^p = (Z_{II}^p)^2 \quad (X_{II}^p, Z_{II}^p \in \mathbb{N})$

$$\begin{aligned} Z_{II}^p &= 2^{p-2+\frac{q}{2}}U + V \qquad \cdots ⑤ \\ X_{II}^p &= 2^{p-2+\frac{q}{2}}U - V \qquad \cdots ⑥ \end{aligned}$$

simultaneous equation:⑤+⑥

$$X_{II}^p + Z_{II}^p = 2^{p-1+\frac{q}{2}}U$$

Corollary 7 $(a+b)^2 + (a-b)^2 = 2\left(a^2+b^2\right)$*:The sum of the squares of two*

$(a, b \in \mathbb{R} \quad a > b)$

And multiplied by 2^{p-2} to both sides.

$$2^{p-2}(a+b)^2 + 2^{p-2}(a-b)^2 = 2^{p-1}\left(a^2+b^2\right)$$

$$\begin{aligned} Z_{II}^p &= 2^{p-2}(a+b)^2 \qquad (Z_{II}^p > X_{II}^p) \\ X_{II}^p &= 2^{p-2}(a-b)^2 \\ 2^{p-1+\frac{q}{2}}U &= 2^{p-1}\left(a^2+b^2\right) \end{aligned}$$

$$\begin{aligned} Z_{II}^p &= 2^{p-2}\left(a^2+b^2+2ab\right) \\ X_{II}^p &= 2^{p-2}\left(a^2+b^2-2ab\right) \\ 2^{\frac{q}{2}}U &= a^2+b^2 \end{aligned}$$

$$\begin{aligned} Z_{II}^p &= 2^{p-2}\left(2^{\frac{q}{2}}U + 2ab\right) = 2^{p-2+\frac{q}{2}}U + 2^{p-1}ab \\ X_{II}^p &= 2^{p-2}\left(2^{\frac{q}{2}}U - 2ab\right) = 2^{p-2+\frac{q}{2}}U - 2^{p-1}ab \end{aligned}$$

In comparison with ⑤,⑥.

$$\begin{aligned} 2^{p-1}ab &= V \\ ab &= \frac{V}{2^{p-1}} \end{aligned}$$

$$\begin{cases} a = \frac{V}{2^{p-1}b} \\ b = \frac{V}{2^{p-1}a} \end{cases}$$

Squaring both sides.

$$\begin{cases} a^2 = \left(\frac{V}{2^{p-1}b}\right)^2 \\ b^2 = \left(\frac{V}{2^{p-1}a}\right)^2 \end{cases}$$

$a^2 + b^2 = 2^{\frac{q}{2}}U$

$$\begin{cases} \left(\frac{V}{2^{p-1}a}\right)^2 + a^2 = 2^{\frac{q}{2}}U \\ \left(\frac{V}{2^{p-1}b}\right)^2 + b^2 = 2^{\frac{q}{2}}U \end{cases}$$

Corollary 8 $(s+t)^2 + (s-t)^2 = 2\left(s^2 + t^2\right)$*:The sum of the squares of two*

$$(s, t \in \mathbb{R} \quad s > t)$$

$$\left(\frac{V}{2^{p-1}b}\right)^2 + b^2 = 2\left(2^{\frac{q}{2}-1}U\right) \qquad \cdots ⑦$$

$b = s \mp t \qquad \frac{V}{2^{p-1}b} = s \pm t \qquad 2^{\frac{q}{2}-1}U = s^2 + t^2$

$$\begin{aligned} \frac{V}{2^{p-1}(s \mp t)} &= s \pm t \qquad (s \neq t) \\ \frac{V}{2^{p-1}} &= s^2 - t^2 \qquad \text{Was added to } 2t^2 \text{to both sides.} \\ \frac{V}{2^{p-1}} + 2t^2 &= s^2 + t^2 \qquad \text{And multiplied by 2 to both sides.} \end{aligned}$$

$$\frac{V}{2^{p-2}} + (2t)^2 = 2\left(2^{\frac{q}{2}-1}U\right) \qquad \cdots ⑧$$

$$\text{If } 2t = s + t, \quad \text{then } t = s. \qquad (s \neq t)$$

Therefore,

$$\begin{aligned} 2t &= s - t \\ 3t &= s \end{aligned}$$

substitute s for ⑧

$(2 \cdot 2t)^2 + (2t)^2 = 2\left(2^{\frac{q}{2}-1}U\right)$

When you assign a ⑧ to ⑦, the following equation is maintained.

$$ab = \frac{V}{2^{p-1}} \qquad a^2 + b^2 = 2^{\frac{q}{2}}U$$

Proof 9

$$ab = K \quad (K \in \mathbb{R})$$

$$\begin{cases} a = \frac{K}{b} \\ b = \frac{K}{a} \end{cases}$$

Squaring both sides.

$$\begin{cases} a^2 = \left(\frac{K}{b}\right)^2 \\ b^2 = \left(\frac{K}{a}\right)^2 \end{cases}$$

$$a^2 + b^2 = L \quad (L \in \mathbb{R})$$

$$\begin{cases} \left(\frac{K}{a}\right)^2 + a^2 = L \\ \left(\frac{K}{b}\right)^2 + b^2 = L \end{cases}$$

Corollary 10 $(s+t)^2 + (s-t)^2 = 2\left(s^2 + t^2\right)$*:The sum of the squares of two*

$$(s, t \in \mathbb{R} \quad s > t)$$

$$\left(\frac{K}{b}\right)^2 + b^2 = L \qquad \cdots ⑨$$

$b = s \mp t \qquad \frac{K}{b} = s \pm t \qquad \frac{L}{2} = s^2 + t^2$

$$\begin{aligned} \frac{K}{(s \mp t)} &= s \pm t \qquad (s \neq t) \\ K &= s^2 - t^2 \qquad \textit{Was added to } 2t^2 \textit{ to both sides.} \\ K + 2t^2 &= s^2 + t^2 \qquad \textit{And multiplied by } 2 \textit{ to both sides.} \end{aligned}$$

$$\begin{aligned} 2K + (2t)^2 &= L \\ \left(2^{\frac{1}{2}} K^{\frac{1}{2}}\right)^2 + (2t)^2 &= L \qquad \cdots ⑩ \end{aligned}$$

If $b = 2^{\frac{1}{2}} K^{\frac{1}{2}}$ *, then* $a = \frac{K}{b} = 2^{-\frac{1}{2}} K^{\frac{1}{2}}$*.* *Therefore,* $ab = K$*.*

From continued.

$$\begin{aligned} \frac{V}{2^{p-1}} &= s^2 - t^2 \\ \frac{V}{2^{p-1}} &= (3t)^2 - t^2 \\ \frac{V}{2^{p-1}} &= 2^3 t^2 \\ V &= 2^{p+2} t^2 = 4 \cdot 2^p t^2 \end{aligned}$$

$$\begin{aligned}
\frac{V}{2^{p-2}} + (2t)^2 &= 2\left(2^{\frac{q}{2}-1}U\right) \quad \text{And multiplied by } 2^{p-2}\text{to both sides.} \\
V + 2^{p-2}\cdot 2^2 t^2 &= 2^{p-2}\left(2^{\frac{q}{2}-1}U\right) \\
2^p t^2 &= 2^{p-2}\left(2^{\frac{q}{2}-1}U\right) - V \in \mathbb{N} \quad (q \in evennumber)
\end{aligned}$$

$$V = 4\cdot 2^p t^2 \qquad V \neq even\ \ number \tag{5}$$

Proposition 11 $p < m \qquad (l+m \geq 2(2p-2) \qquad l \geq m \qquad l, m \in oddnumber)$

$\underline{X_1^p\ ,\ \ Z_1^p \in even\ \ number.}$

$$\begin{aligned}
X^p &= (M-N)^2 \\
&= M^2 + N^2 - 2MN \\
&= 2^l U^2 + 2^m V^2 - 2\cdot 2^{\frac{l+m}{2}} UV \\
&= 2^m\left(2^{l-m}U^2 + V^2 - 2\cdot 2^{\frac{l-m}{2}} UV\right)
\end{aligned}$$

Similarly,

$$\begin{aligned}
Z^p &= (M+N)^2 \\
&= 2^m\left(2^{l-m}U^2 + V^2 + 2\cdot 2^{\frac{l-m}{2}} UV\right)
\end{aligned}$$

$p < m \qquad \left(2^{l-m}U^2 + V^2 + 2\cdot 2^{\frac{l-m}{2}} UV\right) \in \mathbb{N}$

$Y_1^p \in even\ \ number$ so $X_1^p\ ,\ \ Z_1^p \in even\ \ number.$ (6)

2.2 Conditions of (I)

$M = 2^{\frac{l}{2}}c^{\frac{1}{2}} + 2^{\frac{m}{2}}d^{\frac{1}{2}} \qquad N = 2^{\frac{l}{2}}c^{\frac{1}{2}} - 2^{\frac{m}{2}}d^{\frac{1}{2}} \quad (c, d \in odd\ \ number \quad l, m \in \mathbb{N})$

$$\begin{aligned}
X^p &= 2^p X_1^p = (M-N)^2 = \left(2\cdot 2^{\frac{m}{2}}d^{\frac{1}{2}}\right)^2 = 2^2 2^m d \\
Z^p &= 2^p Z_1^p = (M+N)^2 = \left(2\cdot 2^{\frac{l}{2}}c^{\frac{1}{2}}\right)^2 = 2^2 2^l c
\end{aligned}$$

Corollary 12 $(a+b)^2 + (a-b)^2 = 2\left(a^2+b^2\right)$*:The sum of the squares of two*

$(a, b \in \mathbb{R} \quad a > b)$

$$
\begin{aligned}
x^p &= (a+b)^2 \\
y^p &= (a-b)^2 \\
z^p &= 2\left(a^2+b^2\right) \\
(xyz \neq 0)
\end{aligned}
$$

$$
\begin{aligned}
X^p &= (M-N)^2 = (a+b)^2 \\
M-N &= a+b \\
\left(2\cdot 2^{\frac{m}{2}} d^{\frac{1}{2}}\right)^2 &= (a+b)^2 \\
2^2 2^m d &= a^2+b^2+2ab && \text{And multiplied by 2 to both sides.} \\
2^{m+3} d &= 2\left(a^2+b^2\right)+2^2 ab && \left(z^p = 2\left(a^2+b^2\right)\right) \\
2^{m+3} d &= z^p + 2^2 ab \\
2^{m+3} d - 2^2 ab &= z^p && \cdots ⑪
\end{aligned}
$$

$$
MN = 2^{p-2} Y_1^p = \left(2^{\frac{l}{2}} c^{\frac{1}{2}} + 2^{\frac{m}{2}} d^{\frac{1}{2}}\right)\left(2^{\frac{l}{2}} c^{\frac{1}{2}} - 2^{\frac{m}{2}} d^{\frac{1}{2}}\right) = 2^l c - 2^m d
$$

$$
\begin{aligned}
Y^p &= 2^p Y_1^p \\
Y^p = 2^2\left(2^l c - 2^m d\right) &= (a-b)^2 \\
2^2\left(2^l c - 2^m d\right) &= a^2+b^2-2ab && \text{And multiplied by 2 to both sides.} \\
2^3\left(2^l c - 2^m d\right) &= 2\left(a^2+b^2\right) - 2^2 ab && \left(z^p = 2\left(a^2+b^2\right)\right) \\
2^{l+3} c - 2^{m+3} d &= z^p - 2^2 ab \\
2^{l+3} c - 2^{m+3} d + 2^2 ab &= z^p && \cdots ⑫
\end{aligned}
$$

simultaneous equation:⑫−⑪

$$
\begin{aligned}
2^{l+3} c - 2^{m+4} d + 2^3 ab &= 0 \\
2^l c - 2^{m+1} d + ab &= 0 \\
ab &= 2^{m+1} d - 2^l c
\end{aligned}
$$

Remark 13 *Meanwhile, in an inverse relationship,*

$$
\begin{aligned}
X^p &= (a-b)^2 \\
2^{m+3} d + 2^2 ab &= z^p && \cdots ⑬ \\
Y^p &= (a+b)^2 \\
2^{l+3} c - 2^{m+3} d - 2^2 ab &= z^p && \cdots ⑭
\end{aligned}
$$

*simultaneous equation:*⑬−⑭

$$
\begin{aligned}
-2^{l+3} c + 2^{m+4} d + 2^3 ab &= 0 \\
-2^l c + 2^{m+1} d + ab &= 0 \\
ab &= 2^l c - 2^{m+1} d
\end{aligned}
$$

$$\text{put} \quad 2^{m+1}d - 2^l c = e$$
$$ab = e$$

$$\begin{cases} a = \frac{e}{b} \\ b = \frac{e}{a} \end{cases}$$

Squaring both sides.

$$\begin{cases} a^2 = \left(\frac{e}{b}\right)^2 \\ b^2 = \left(\frac{e}{a}\right)^2 \end{cases}$$

$$2\left(a^2 + b^2\right) = z^p$$

$$\begin{cases} 2\left(\left(\frac{e}{a}\right)^2 + a^2\right) = z^p \\ 2\left(\left(\frac{e}{b}\right)^2 + b^2\right) = z^p \end{cases} \qquad \text{And multiplied by 2 to both sides.}$$

Corollary 14 $(s+t)^2 + (s-t)^2 = 2\left(s^2 + t^2\right)$*:The sum of the squares of two*

$$(s, t \in \mathbb{R} \quad s > t)$$

$$\left(\frac{2e}{b}\right)^2 + (2b)^2 = 2z^p \qquad \cdots ⑮$$

$2b = s \mp t \qquad \frac{2e}{b} = s \pm t \qquad z^p = s^2 + t^2$

$$\begin{aligned} \frac{2e}{b} &= s \pm t && \text{And multiplied by } \tfrac{1}{2} \text{ to both sides.} \\ \frac{2e}{2b} &= \frac{s \pm t}{2} \\ \frac{2e}{s \mp t} &= \frac{s \pm t}{2} && (s \neq t) \\ 2^2 e &= s^2 - t^2 && \text{Was added to } 2t^2 \text{to both sides.} \\ 2^2 e + 2t^2 &= s^2 + t^2 && \text{And multiplied by 2 to both sides.} \\ 2^3 e + (2t)^2 &= 2z^p && \cdots ⑯ \end{aligned}$$

$$\text{If } 2t = s + t, \quad \text{then } t = s. \qquad (s \neq t)$$

Therefore,

$$\begin{aligned} 2t &= s - t \\ 3t &= s \end{aligned}$$

When you assign a ⑯ to ⑮, the following equation is maintained.

$$ab = e \qquad a^2 + b^2 = \frac{z^p}{2}$$

$$
\begin{aligned}
2^2 e &= s^2 - t^2 \\
2^2 e &= (3t)^2 - t^2 \\
2^2 e &= 2^3 t^2 \\
e &= 2t^2 \qquad \cdots ⑰
\end{aligned}
$$

$$
\begin{aligned}
2^3 e + (2t)^2 &= 2z^p \qquad Substitute ⑰. \\
2^3 e &= 2z^p - 2e
\end{aligned}
$$

$e = 2^{m+1} d - 2^l c$

$$
\begin{aligned}
X^p &= 2^p X_1^p = 2^2 2^m d \\
Z^p &= 2^p Z_1^p = 2^2 2^l c \\
2^{p-2} Y_1^p &= 2^l c - 2^m d
\end{aligned}
$$

Proposition 15 $l \geq p-1$, $m \geq p-1$ $\qquad (c, d \in odd\ \ number \quad l, m \in \mathbb{N})$

$\underline{X_1^p \ , \ Z_1^p \in even\ \ number}$

$$
\begin{aligned}
2 + l &\geq p + 1 \\
2 + m &\geq p + 1
\end{aligned}
$$

$Y_1^p \in even\ \ number$ so X_1^p , $Z_1^p \in even\ \ number.$ (7)

Proposition 16 $l = p-2$, $m \geq p-2$ $\qquad (c, d \in odd\ \ number \quad l, m \in \mathbb{N})$

$\underline{e = 2^{p-2}\,(oddnumber)}$

$$
\begin{aligned}
e &= 2^{m+1} d - 2^l c \\
&= 2^{m+1} d - 2^{p-2} c \\
&= 2^{p-2} \left(2^{m+3-p} d - c \right)
\end{aligned}
$$

$m + 3 \geq p + 1$ $\qquad 2^{m+3-p} d \in even\ \ number$

$$
\begin{aligned}
e &= 2^{p-2}\,(odd\ \ number) \\
e &= 2^{p-2} w \qquad (\text{put w}\in odd\ \ number)
\end{aligned}
$$

$$
2^3 e = 2z^p - 2e \qquad \left(e = 2^{p-2} w \right)
$$

$$
2^{p+1} w = 2z^p - 2^{p-1} w
$$

$2^3 e = 2^{p+1} w \equiv 0 \pmod{2^p}$

2^{p-1} because there are $2n \pm 1(w)$,
$2^{p-1} \cdot 2n \pm 2^{p-1} = 2^p n \pm 2^{p-1}$

$2e = 2^{p-1} w \equiv \pm 2^{p-1} \pmod{2^p}$

z^p is condition of odd,
$2z^p \equiv \pm (4n+2) \pmod{2^p}$
Can not offset the remainder $\pm 2^{p-1}$ so multiple of 4.

z^p is condition of even,
$2z^p \equiv 0 \pmod{2^p}$
Can not offset the remainder $\pm 2^{p-1}$.

Therefore, $e = 2^{p-2}\,(oddnumber)$ is not hold. (8)

$$\begin{aligned} X^p &= 2^p X_1^p = 2^2 2^m d \\ Z^p &= 2^p Z_1^p = 2^2 2^l c \\ 2^{p-2} Y_1^p &= 2^l c - 2^m d \end{aligned}$$

$l \geq p-1 \qquad m = p-2$

Condition $p < l < 2p-2$ is not hold. $(Z_1^p \in even\ \ number)$

Proposition 17 $l \geq 2p{-}2 \qquad m = p{-}2 \qquad (c, d \in odd\ \ number \quad l, m \in \mathbb{N})$

$\underline{2^{p+1} w = 2z^p - 2^{p-1} w \quad does\ not\ hold.\ (w \in odd\ \ number)}$

$$l = 2p - 2 + k \quad (k = 0\ \ or\ \ \mathbb{N})$$

$$\begin{aligned} e &= 2^{m+1} d - 2^l c \\ &= 2^{p-1} d - 2^{2p-2+k} c \\ &= 2^{p-1} \left(d - 2^{p-1+k} c \right) \end{aligned}$$

$$\begin{aligned} h &= d - 2^{p-1+k} c \\ e &= 2^{p-1} h \qquad (h \in odd\ \ number) \end{aligned}$$

$2^3 e = 2z^p - 2e \qquad (e = 2^{p-1} h \ ,\ \ z^p = 2^p Z_1^p)$

$$\begin{aligned} 2^{p+2} h &= 2^{p+1} Z_1^p - 2^p h \qquad \text{By removing the } 2^p \text{ from both sides,} \\ 2^2 h &= 2 Z_1^p - h \end{aligned}$$

This is contradictory to that h is odd. (9)

3 As a result of the above.

$Y_1^p \in even\ number$ so X_1^p , $Z_1^p \in even\ number$;(1),(6),(7)
The contradictory to assumption;(2),(4),(5),(8),(9)

By referring to the (3),

$$U_{II}^p = Z_{II}^p + X_{II}^p \qquad V_{II}^p + X_{II}^p = Z_{II}^p$$

$$(2U_{II})^p = (2Z_{II})^p + (2X_{II})^p \qquad (2V_{II})^p + (2X_{II})^p = (2Z_{II})^p$$

$$(2Z_{II})^p < z^p = (2Z_I)^p \qquad (2X_{II})^p < X^p = (2X_I)^p$$

Thus the lemma has been shown.

$$x^n + y^n \neq z^n \qquad (xyz \neq 0 \quad n \geq 3)$$