The idea of the Arithmetica

Hajime Mashima

July 3, 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 $\quad X,Y,Z \in \mathbb{N} \quad$ 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 $\quad h, i \in \mathbb{N})$
$M = 2^{\frac{h}{2}} c^{\frac{1}{2}} + 2^{\frac{i}{2}} d^{\frac{1}{2}} \qquad N = 2^{\frac{h}{2}} c^{\frac{1}{2}} - 2^{\frac{i}{2}} d^{\frac{1}{2}} \qquad$ (I)

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

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

$MN = 2^{p-2}Y_1^p = 2^{\frac{l+m}{2}}UV \in \mathbb{N}$

M, N because irrational both.therefore, l, m is 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 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.

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

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

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

Lemma 2 *If not satisfied with the exception of these conditions, infinite descent method can be applied.*

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

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

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

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

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).

$$U = Z_{II}^p + X_{II}^p = rf \qquad \cdots ③$$
$$V = Z_{II}^p - X_{II}^p = rg \qquad \cdots ④$$
$$(U, V \in odd\ \ number \qquad f, g \in odd\ \ number)$$

simultaneous equation:③±④

$$2Z_{II}^p = r\,(f+g)$$
$$2X_{II}^p = r\,(f-g)$$

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

Theorem 3 $(Y_1^p = UV)$ *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.

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

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

It is equivalent to X_1^p because it is odd number.

$$MN = 2^{p-2} X_1^p = 2^{\frac{l+m}{2}} UV \qquad (p = \tfrac{l+m}{2} + 2 \qquad X_1^p = UV)$$

Proposition 4 $x^p + y^p = z^p$
x^p(or y^p) and z^p is a square number, both when this condition is satisfied.

Put $e,\ f,\ c \in \mathbb{N}$ *prime number* $= p \geq 3$

$$e^p + f^p = c^{2p}$$

Theorem 5

$$(a+b)^2 + (a-b)^2 = 2(a^2+b^2)$$

$$(M-N)^2 + 2^2MN = (M+N)^2$$

Corollary 6

$$st = \left(\frac{(st)^{\frac{1}{2}}(s-t)}{s+t}\right)^2 + \left(\frac{2st}{s+t}\right)^2$$

$$st = \left(\frac{s+t}{2}\right)^2 - \left(\frac{s-t}{2}\right)^2$$

Put $st = a+b = M-N$

$$a = \left(\frac{(st)^{\frac{1}{2}}(s-t)}{s+t}\right)^2 \qquad b = \left(\frac{2st}{s+t}\right)^2$$

$$M = \left(\frac{s+t}{2}\right)^2 \qquad N = \left(\frac{s-t}{2}\right)^2 \quad \cdots ⑤$$

Put $2^2MN = f^p$
$(M-N)^2 = e^p$
$(M+N)^2 = c^{2p}$

$$M - N = e^{\frac{p}{2}} \quad \cdots ⑥ \qquad M + N = c^p \quad \cdots ⑦$$

⑦ ± ⑥

$$M = \frac{c^p + e^{\frac{p}{2}}}{2} \qquad N = \frac{c^p - e^{\frac{p}{2}}}{2} \quad \cdots ⑧$$

$$e^p = (M-N)^2 = (st)^2 = \left(\frac{s^2+t^2}{2}\right)^2 - \left(\frac{s^2-t^2}{2}\right)^2$$

$$f^{\frac{p}{2}} = a-b = \left(\frac{(st)^{\frac{1}{2}}(s-t)}{s+t}\right)^2 - \left(\frac{2st}{s+t}\right)^2 = \frac{st(s-t)^2 - 2^2(st)^2}{(s+t)^2} \quad \cdots ⑨$$

By referring to the ⑤ and ⑧,

$$\left(\frac{s+t}{2}\right)^2 = \frac{c^p + e^{\frac{p}{2}}}{2} \qquad \left(\frac{s-t}{2}\right)^2 = \frac{c^p - e^{\frac{p}{2}}}{2}$$

$$\frac{s+t}{2} = \sqrt{\frac{c^p + e^{\frac{p}{2}}}{2}} \quad \cdots ⑩ \qquad \frac{s-t}{2} = \sqrt{\frac{c^p - e^{\frac{p}{2}}}{2}} \quad \cdots ⑪$$

⑩±⑪

$$s = \sqrt{\frac{c^p + e^{\frac{p}{2}}}{2}} + \sqrt{\frac{c^p - e^{\frac{p}{2}}}{2}} \qquad t = \sqrt{\frac{c^p + e^{\frac{p}{2}}}{2}} - \sqrt{\frac{c^p - e^{\frac{p}{2}}}{2}}$$

$$\begin{aligned} s^2 &= \frac{c^p + e^{\frac{p}{2}}}{2} + \frac{c^p - e^{\frac{p}{2}}}{2} + 2\sqrt{\frac{c^{2p} - e^p}{2^2}} \\ &= c^p + \sqrt{c^{2p} - e^p} \end{aligned}$$

$$\begin{aligned} t^2 &= \frac{c^p + e^{\frac{p}{2}}}{2} + \frac{c^p - e^{\frac{p}{2}}}{2} - 2\sqrt{\frac{c^{2p} - e^p}{2^2}} \\ &= c^p - \sqrt{c^{2p} - e^p} \end{aligned}$$

$$s^2 - t^2 = 2\sqrt{c^{2p} - e^p} = 2f^{\frac{p}{2}} \qquad s^2 + t^2 = 2c^p \qquad \cdots ⑫$$

By referring to the ⑨,⑫,

$$\begin{aligned} f^{\frac{p}{2}} &= \frac{st(s-t)^2 - 2^2(st)^2}{(s+t)^2} \\ &= \frac{st\left(s^2+t^2-2st\right) - 2^2(st)^2}{s^2+t^2+2st} \\ &= \frac{e^{\frac{p}{2}}\left(2c^p - 2e^{\frac{p}{2}}\right) - 2^2e^p}{2c^p + 2e^{\frac{p}{2}}} \\ &= \frac{e^{\frac{p}{2}}\left(c^p - e^{\frac{p}{2}}\right) - 2e^p}{c^p + e^{\frac{p}{2}}} \\ &= \frac{e^{\frac{p}{2}}c^p - 3e^p}{c^p + e^{\frac{p}{2}}} \end{aligned}$$

$$
\begin{aligned}
f^p &= \left(\frac{e^{\frac{p}{2}}c^p - 3e^p}{c^p + e^{\frac{p}{2}}}\right)^2 \\
&= e^p\left(\frac{c^p - 3e^{\frac{p}{2}}}{c^p + e^{\frac{p}{2}}}\right)^2 \\
&= e^p\left(\frac{\left(c^p - 3e^{\frac{p}{2}}\right)\left(c^p - e^{\frac{p}{2}}\right)}{\left(c^p + e^{\frac{p}{2}}\right)\left(c^p - e^{\frac{p}{2}}\right)}\right)^2 \\
&= e^p\left(\frac{\left(c^p - 3e^{\frac{p}{2}}\right)\left(c^p - e^{\frac{p}{2}}\right)}{c^{2p} - e^p}\right)^2 \\
&= \frac{e^p\left(c^{2p} + 3e^p - 4e^{\frac{p}{2}}c^p\right)^2}{\left(c^{2p} - e^p\right)^2} \\
&= \frac{e^p}{\left(c^{2p} - e^p\right)^2}\left(\left(c^{2p} + 3e^p\right)^2 + 4^2e^pc^{2p} - 2\cdot 4e^{\frac{p}{2}}c^p\left(c^{2p} + 3e^p\right)\right)
\end{aligned}
$$

if f^p, c^p is a natural number, e must be a square number.

$$e^p + f^p = c^{2p} \qquad \cdots ⑭$$

Corollary 7 *When the following equation is satisfied, x^p and z^p is a square number.*

$$x^p + y^p = z^p \quad (x,\ y \text{ and } z \text{ are disjoint.}) \qquad (x^p\ ,\ y^p\ ,\ z^p \in \mathbb{N})$$

And multiplied by z^p to both sides.

$$z^px^p + z^py^p = z^{2p}$$

By applying the ⑭, since "z^px^p" is also a square number,

$$x^p = \left(x_1^p\right)^2\ ,\ z^p = \left(z_1^p\right)^2$$

$$\left(x_1^2\right)^p + y^p = \left(z_1^2\right)^p \quad (x_1, \text{ y and } z_1 \text{ are disjoint.})$$

By referring to the (2),

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

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

$$(2Z_{II})^p < Z^p = (2Z_1)^p \qquad (2X_{II})^p < X^p = (2X_1)^p$$

Thus the lemma has been shown.

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