# Sophie-Germain prime $p_s$ and Fermat's Last Theory

H. Tohmori 2021.11.09

## Abstract

Sophie-Germain did not prove Fermat's Last Theorem (FLT) itself, but she studied the conditions for FLT to hold using Sophie-Germain prime $p_s$ and prime $(2p_s+1)$. But Algebra at the time of Sophie-Germain can prove that FLT holds for Fermat's equation with an exponent of prime $p_s$. Below is an overview.

If Fermat's equation with an exponent of prime $p_s$ holds in arithmetic operation, it always holds in modulo operation by prime $(2p_s+1)$.

But, even if the Fermat's equation holds in modulo operation by prime $(2p_s+1)$, it does not necessarily hold in arithmetic operation.

However, the Fermat's equation never holds in arithmetic operations unless it holds in modulo operation by prime $(2p_s+1)$.

Therefore, by proving that Fermat's equation with an exponent of prime $p_s$ does not hold in modulo operation by prime $(2p_s+1)$, it is proved that the Fermat's equation does not hold in arithmetic operation.

## 1. Introduction

Fermat's equation with an exponent of prime $p_s$ is as follows.

$p_s$ is Sophie-Germain prime such that $(2p_s+1)$ is also prime.

Natural number $A$, $B$ and $C$ are coprime.

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

$\left(\frac{Q}{R}\right)$ is defined as remainder (modulo) when natural number Q is modulo operated by natural number $R$.

The notation in the center is correct, but it is written as shown on the right side.

$$\left(\frac{QS}{RT}\right)=\left(\frac{\left(\frac{Q}{RT}\right)\left(\frac{S}{RT}\right)}{RT}\right)=\left(\frac{Q}{RT}\right)\left(\frac{S}{RT}\right) \qquad \left(\frac{Q\pm S}{RT}\right)=\left(\frac{\left(\frac{Q}{RT}\right)\pm\left(\frac{S}{RT}\right)}{RT}\right)=\left(\frac{Q}{RT}\right)\pm\left(\frac{S}{RT}\right)$$

## 2. Complementarity of modulo operation

Following two modulo operation are complementary to each other.

Natural number $X$, $Y$, $B$ and $C$ are coprime to each other.

Neither natural number $C$ and $B$ contains prime $(2p_s+1)$.

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

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

That is, as shown below, when one of above two equations is not $0$, the other equation is $0$.

$$\left(\frac{C^{2p_s}}{2p_s+1}\right)=\left(\frac{C^{p_s}}{2p_s+1}\right)^2=1 \quad \left(\frac{C^{p_s}}{2p_s+1}\right)=\pm1 \quad \left(\frac{B^{2p_s}}{2p_s+1}\right)=\left(\frac{B^{p_s}}{2p_s+1}\right)^2=1 \quad \left(\frac{B^{p_s}}{2p_s+1}\right)=\pm1$$

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

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

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

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

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

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

As can be seen from the above, following equation (2.1) holds complementarily regardless of natural number $C$ and $B$.

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

# 3. Fermat's equation with an exponent of prime number $p_s$

## 3.1 When neither natural number $C$ and $B$ contains prime $(2p_s+1)$

Above equation (1.1) can be rewritten to following equation (3.1.1).

At that time, there are always natural number $X$ and $Y$ that holds following equations (3.1.1) and (3.1.2).

From equation (2.1) in previous section, either of natural numbers $X$ and $Y$ contains prime $(2p_s+1)$.

Natural number $X$, $Y$, $B$ and $C$ are coprime to each other.

$$A^{p_s} = X = C^{p_s} - B^{p_s} \tag{3.1.1}$$

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

When natural number $Y$ contains prime $(2p_s+1)$, equation (3.1.3) holds, as shown below.

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

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

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

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

Since natural number $X$ and $C$ are coprime to each other, following equation (3.1.3) must hold.

Natural number $E$ is coprime to natural number $C$ and $B$.

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

Conversely, when natural number $X$, that is, natural number $E$ contains prime $(2p_s+1)$, equation (3.1.4) holds, as shown below.

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

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

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

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

Since natural number $Y$ and $C$ are coprime to each other, following equation (3.1.4) must hold.

Natural number $F$ and $C$ are coprime to each other.

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

From the above, equations (3.1.1) and (3.1.2) can be rewritten into following two equations (3.1.5) and (3.1.6).

Natural number $F$, $E$, $C$ and $B$ are coprime to each other.

Either of natural numbers $F$ and $E$ contains prime $(2p+1)$.

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

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

Then, following equation must hold to hold Fermat's equation (1.1).

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

However, there is no natural number $A$ that holds above equation.

Therefore, when neither natural number $C$ and $B$ contains prime $(2p_s+1)$, there are no natural numbers $A$, $B$ and $C$ that hold Fermat's equation (1.1).

## 3.2 When neither natural number $A$ and $B$ contains prime $(2p_s+1)$

There are always natural number $U$ and $V$ that holds following equations (3.2.1) and (3.2.2).

Natural number $U$, $V$, $A$ and $B$ are coprime to each other.

$$A^{p_s}-B^{p_s}=U \tag{3.2.1}$$

$$A^{p_s}+B^{p_s}=V=C^{p_s} \tag{3.2.2}$$

From the similarity with the previous section **3.1**, following equations (3.2.3) and (3.2.4) hold.

Natural numbers $G$, $H$, $A$ and $B$ are coprime to each other.

Either of natural numbers $G$ and $H$ contains prime $(2p_s+1)$.

Natural numbers $A$ and $B$ do not contain prime $(2p_s+1)$.

$$A^{p_s}-B^{p_s}=2G^{p_s}=U \tag{3.2.3}$$

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

However, there are no natural numbers $C$ that holds above equation $(3.2.4)$.

Therefore, when neither natural number $A$ and $B$ contains prime $(2p_s + 1)$, there are no natural numbers $A$, $B$ and $C$ that hold Fermat's equation $(1.1)$.

As mentioned above, there are no natural numbers $A$, $B$ and $C$ that hold Fermat's equation $(1.1)$ with an exponent of prime $p_s$.

Therefore, Fermat's Last Theory holds for Fermat's equation with an exponent of prime $p_s$.

## 5. Conclusion

Fermat's equation with an exponent of prime $p_s$ does not hold in modulo operation by prime $(2p_s + 1)$.

Then, the Fermat's equation never holds in arithmetic operations.

Therefore, there are no natural numbers $A$, $B$ and $C$ that hold the Fermat's equation.

That is, Fermat's Last Theorem holds for Fermat's equation with an exponent of prime $p_s$.

## 6. References

[1] L. Riddle, "Sophie Germain and Fermat's Last Theorem," Agnes Scott College, 2009.
http://www.agnesscott.edu/Lriddle/women/germain-FLT/SGandFLT.htm

[2] Colleen-Alkalay-Houlihan, "Sophie Germain and Special Cases of Fermat's Last Theorem"
https://www.math.mcgill.ca/darmon/courses/12-13/nt/projects/Colleen-Alkalay-Houlihan.pdf