A proof of Fermat's Last Theorem (FLT)

H. Tohmori 2024.04.21

Abstract

If Fermat's equation with an exponent of prime p holds in arithmetic operation, it always holds in modulus operation by factor $(2p+1)$ regardless of whether factor $(2p+1)$ is prime or not.

But, even if Fermat's equation holds in modulus operation by factor $(2p+1)$, it does not necessarily hold in arithmetic operation.

However, Fermat's equation never holds in arithmetic operations unless it holds in modulus operation by factor $(2p+1)$.

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

As a result, FLT is proved.

1. Introduction

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

Natural number A, B and C are coprime.

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

$\left(\frac{Q}{R}\right)$ 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. The remainders of the factors $(2p+1)$ is p

individual

Below, the following equation (2.1) is proved regardless of whether the factor $(2p+1)$ is prime or not.

The natural numbers A and B are prime to each other, and neither contains any factors $(2p+1)$.

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

The following equation (2.2) holds.

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

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

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

As can be seen from the above, the remainder $\left(\frac{D^2}{2p+1}\right)$ due to the factors $(2p+1)$ of D^2 is p individual.

$$i=1\sim p$$

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

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

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

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

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

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

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

As described above, the remainder $\left(\frac{E^2}{2p+1}\right)$ due to the factors $(2p+1)$ of E^2 is p individual as follows.

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

Then, each of the above remainders $\left(\frac{D^2}{2p+1}\right)$ always corresponds to one of the above remainders $\left(\frac{E^2}{2p+1}\right)$, i.e., the following equation holds.

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

Therefore, the above remainder (2.2) is rewritten as follows, and the equation (2.3) is established.

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

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

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

3. The equation (2.1) holds even when the factor (2p+1) is not prime.

In the following, it is proved that the equation (2.1) holds regardless of whether the factor $(2p+1)$ is prime or not.

3.1 Any prime number p is denoted as p_+ or p_-.

The formula for the sum of squares of natural numbers is as follows.

$$\sum_{i=1}^{k} i^2=1+2^2+3^2+\cdots+(k-2)^2+(k-1)^2+k^2=k(K+1)(2k+1)/6$$

Since the sum of squares of natural numbers is an integer, $k(K+1)(2k+1)$ is divisible by number 6.

When $p_k=2k+1$ is prime number, $(2k+1)$ is not divisible by number 6.

At that time, k or $k+1$ is divisible by number 3 because either of them is even number.

As a result, every prime number p_k is included in following two series.

m is natural number.

$k=3m \qquad p_+=6m+1$

$k+1=3m \qquad p_-=6m-1$

Therefore, every prime number p is denoted as prime number p_+ or p_-.

3.2. The equation (2.1) holds when $p = p_+$

$$p_+ = 6m + 1$$

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

When the modulus operation is performed on the factor $(2p_+ + 1)$, the squared term containing p_i does not appear.

The sum of the squared terms including p_i is subtracted from the sum of the squared terms.

p_i is prime $\quad p_{i-1} < p_i < p_{i+1} \quad$ i and n are natural number.

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

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

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

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

Duplicates of the squared terms including p_i and p_j are calculated.

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

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

$$\begin{aligned}
(p_i p_j)^2 + (2p_i p_j)^2 + (3p_i p_j)^2 + \cdots + \left(l_{ij} p_i p_j\right)^2 &= l_{ij}\left(l_{ij} + 1\right)\left(2l_{ij} + 1\right)\left(p_i p_j\right)^2/6 \\
&= l_{ij}\left(l_{ij} + 1\right)\left(p_1{}^{n_1} p_2{}^{n_2} p_3{}^{n_3} \dots p_i{}^{n_i - 1} \dots p_j{}^{n_j - 1} \dots . p_n{}^{n_n}\right)\left(p_i p_j\right)^2/6 \\
&= l_{ij}\left(l_{ij} + 1\right)p_i p_j(p_1{}^{n_1} p_2{}^{n_2} p_3{}^{n_3} \dots p_i{}^{n_i} \dots p_n{}^{n_n})/6 \\
&= l_{ij}\left(l_{ij} + 1\right)p_i p_j(2p_+ + 1)/6 \\
&= l_{ij}\left(l_{ij} + 1\right)p_i p_j(4m + 1)/2
\end{aligned}$$

The equation (2.3) holds as follows.

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

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

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

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

The equation (2.1) holds as follows.

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

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

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

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

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

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

$$= 0$$

It is illustrated below.

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

$A = 2 \quad B = 1 \quad p_+ = 19 \quad 2p_+ + 1 = 39$

Then the equality (2.3) is as follows.

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

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

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

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

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

$$2^2 = 2^2$$

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

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

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

$$(2^2)^5 = 7^2 + 39 \times 25$$

$$(2^2)^6 = 14^2 + 39 \times 100$$

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

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

$p_+ = 37 \quad (2p_+ + 1) = 75 = 3 \times 5^2 \qquad p_1 = 3 \quad p_2 = 5 \quad n = 2$
$A = 2 \qquad B = 1 \qquad p_+ = 37 \qquad 2p_+ + 1 = 75$
Then the equality (2.3) is as follows.

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

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

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

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

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

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

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

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

3.3. Equation (2.1) holds when $p = p_-$

$$p_- = 6m - 1$$
$$2p_- + 1 = 2(6m-1) + 1 = 12m - 1$$

Then, the right side of the above equation (2.3) is rewritten as follows.

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

$$= \left(\frac{(6m-1)(6m)(12m-1)/6}{12m-1}\right)$$

$$= \left(\frac{(6m-1)(m)(12m-1)}{12m-1}\right) = 0$$

3.3.1 If the factor $(2p_- + 1)$ is prime, then the equation (2.1) holds.

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

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

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

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

3.3.2 Even when the factor $(2p_- + 1)$ is not prime, the equation (2.1) holds as follows.

When the modulus operation is performed on the factor $(2p_- + 1)$, the squared term containing p_i does not appear.

The sum of the squared terms including p_i is subtracted from the sum of the squared terms.

$$p_i \geq 5 \text{ is prime} \qquad p_{i-1} < p_i < p_{i+1} \qquad i = 1 \sim n$$

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

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

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

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

Since $p_i \geq 5$. $l_i(l_i + 1)$ is multiple of number 6.

Duplicates of the squared terms including p_i and p_j are calculated.

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

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

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

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

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

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

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

等式(2.3)は次の如く書き換えられる.

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

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

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

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

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

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

$$= 0$$

Naturally, the equation (2.1) holds.

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

Examples where the factor $(2p_- + 1)$ is not prime are shown below.

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

$A = 2 \quad B = 1$

$$\left(\frac{\sum_{i=1}^{p_-} A^{2(p_- - i)}B^{2(i-1)}}{2p_- + 1}\right) = \left(\frac{\sum_{i=1}^{p_-} 2^{2(p_- - i)}}{2p_- + 1}\right) - \left(\frac{\sum_{i=1}^{n} l_i(l_i+1)p_i(2p_-+1)}{6(2p_-+1)}\right)$$

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

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

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

$$2^2 = 2^2$$
$$(2^2)^2 = 4^2$$
$$(2^2)^3 = 8^2$$
$$(2^2)^4 = 16^2$$
$$(2^2)^5 = 3^2 + 35 \times 29$$
$$(2^2)^6 = 6^2 + 35 \times 116$$
$$(2^2)^7 = 12^2 + 35 \times 464$$
$$(2^2)^8 = 11^2 + 35 \times 1869$$
$$(2^2)^9 = 13^2 + 35 \times 7485$$
$$(2^2)^{10} = 9^2 + 35 \times 29957$$
$$(2^2)^{11} = 17^2 + 35 \times 119829$$
$$(2^2)^{12} = 1^2 + 35 \times 479349$$

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

$$3^2 = 3^2$$
$$(3^2)^2 = 9^2$$
$$(3^2)^3 = 8^2 + 35 \times 19$$
$$(3^2)^4 = 11^2 + 35 \times 184$$
$$(3^2)^5 = 2^2 + 35 \times 1687$$
$$(3^2)^6 = 6^2 + 35 \times 116$$
$$(3^2)^7 = 17^2 + 35 \times 15183$$
$$(3^2)^8 = 16^2 + 35 \times 1869$$
$$(3^2)^9 = 13^2 + 35 \times 11{,}069{,}152$$
$$(3^2)^{10} = 4^2 + 35 \times 99{,}622{,}411$$
$$(3^2)^{11} = 12^2 + 35 \times 896{,}601{,}699$$
$$(3^2)^{12} = 1^2 + 35 \times 8{,}069{,}415{,}328$$

As described above, the equation (2.1) holds regardless of whether the factor $(2p + 1)$ is prime or not.

4. Fermat's equation does not hold in modulus

operation by the factor (2p+1).

Natural numbers U and V that satisfy following equation always exist.

Natural numbers U, V, A and B are relatively prime.

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

The above equation (2.1) is transformed as follows.

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

Either natural number U or V contains factor $(2p+1)$.

When natural number U contains factor $(2p+1)$, following equation must hold for Fermat's equation (1.1) to hold.

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

However, it is shown below that the above equation does not hold.

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

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

As shown above, Fermat's equation (1.1) does not hold in the modulo operation using the factor $(2p+1)$.

Therefore, there are no natural numbers A, B and C that satisfy Fermat's equation (1.1) in arithmetic operations.

If the factor $(2p+1)$ is not prime, the product $p_1p_2 = (2p+1)$ of prime p_1 and prime p_2, then the following can be considered.

It is possible that natural number U contains prime p_1 and natural number V contains prime p_2 or vice versa.

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

The following proves that the above case is impossible.

Since the prime number p_1 is included in either the natural numbers U or V, the following equality must hold regardless of the natural numbers A and B.

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

However, as shown below, the above equation does not hold regardless of the natural numbers A and B.

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

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

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

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

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

That is, the product $p_1p_2 = (2p+1)$ must be contained in either the natural numbers U or V.

Next, it is proved that the following equality holds regardless of the natural numbers A and B.

$$\left(\frac{UV}{p_1p_2}\right) = 0$$

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

$$= \left(\frac{A^{(p_2(p_1-1)+p_2-1)}}{p_1p_2}\right) - \left(\frac{B^{(p_2(p_1-1)+p_2-1)}}{p_1p_2}\right)$$

$$= \left(\frac{A^{p_2(p_1-1)}}{p_1p_2}\right)\left(\frac{A^{p_2-1)}}{p_1p_2}\right) - \left(\frac{B^{p_2(p_1-1)}}{p_1p_2}\right)\left(\frac{B^{p_2-1)}}{p_1p_2}\right)$$

$$\left(\frac{A^{p_2(p_1-1)}}{p_1p_2}\right) = \left(\frac{B^{p_2(p_1-1)}}{p_1p_2}\right) = \left(\frac{1}{p_1p_2}\right)$$

$$\left(\frac{A^{(p_2-1)}}{p_1p_2}\right) = \left(\frac{B^{(p_2-1)}}{p_1p_2}\right) = \left(\frac{1}{p_1p_2}\right)$$

$$= 0$$

It is proved by mathematical induction that the above holds true in the following cases as well. The proof is omitted here.

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

Therefore, FLT is proved when neither natural number A nor

B contains prime $(2p+1)$.
Also, FLT is proved in the same way as above even when neither natural number B nor C contains factor $(2p+1)$.

5. Conclusion

Fermat's equation with an exponent of prime p does not hold in modulo operation with prime $(2p+1)$.
Then, Fermat's equation never holds in arithmetic operations.
Therefore, there are no natural numbers A, B, and C that hold Fermat's equation.
That is, Fermat's Last Theorem holds for Fermat's equation with an exponent of prime p.

6. References

[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.