

フェルマーの小定理の証明

愛犬ベルのために

最新 2023 年 7 月 5 日

はじめに

私は、フェルマーの最終定理を BBS「数の不思議世界」で、壊れた扉さんと議論してきました。なかなか、私の掲示板の二項定理を使った $a^n - 1^n$ を前進できなかったのですが、壊れた扉さんの「 ${}_nC_r$ は n が素数のとき n の倍数である」ということで、ついに解決に至りました。

そして、BBS「出会いの泉」で、KY 様より、フェルマーの小定理ではないかと指摘されましたので、改題しました。(2023-4-9)

更新履歴

2021.7.24 新規作成

2021.8.14 これらを足すの指数修正

2021.8.15 n を奇数から奇素数に変更

2023.4.9 [フェルマーの小定理の証明] と改題し、追記

2023.7.5 n を奇素数から素数に変更

1 二項定理

1.1 数の n 乗を二項定理で表す

$$2^n = (1+1)^n = {}_nC_0 1^n 1^0 + {}_nC_1 1^{n-1} 1^1 + {}_nC_2 1^{n-2} 1^2 + \cdots + {}_nC_{n-1} 1^{n-n+1} 1^{n-1} + {}_nC_n 1^{n-n} 1^n$$

$$2^n = (1+1)^n = {}_nC_0 1^n + {}_nC_1 1^{n-1} + {}_nC_2 1^{n-2} + \cdots + {}_nC_{n-1} 1^{n-n+1} + {}_nC_n 1^{n-n}$$

同様に、

$$3^n = (2+1)^n = {}_nC_0 2^n + {}_nC_1 2^{n-1} + {}_nC_2 2^{n-2} + \cdots + {}_nC_{n-1} 2^{n-n+1} + {}_nC_n 2^{n-n}$$

$$4^n = (3+1)^n = {}_nC_0 3^n + {}_nC_1 3^{n-1} + {}_nC_2 3^{n-2} + \cdots + {}_nC_{n-1} 3^{n-n+1} + {}_nC_n 3^{n-n}$$

$$5^n = (4+1)^n = {}_nC_0 4^n + {}_nC_1 4^{n-1} + {}_nC_2 4^{n-2} + \cdots + {}_nC_{n-1} 4^{n-n+1} + {}_nC_n 4^{n-n}$$

$$6^n = (5+1)^n = {}_nC_0 5^n + {}_nC_1 5^{n-1} + {}_nC_2 5^{n-2} + \cdots + {}_nC_{n-1} 5^{n-n+1} + {}_nC_n 5^{n-n}$$

1.2 これらを足す

$$\begin{aligned}
 2^n &= (1+1)^n = {}_n C_0 1^n + {}_n C_1 1^{n-1} + {}_n C_2 1^{n-2} + \cdots + {}_n C_{n-1} 1^{n-n+1} + {}_n C_n 1^{n-n} \\
 3^n &= (2+1)^n = {}_n C_0 2^n + {}_n C_1 2^{n-1} + {}_n C_2 2^{n-2} + \cdots + {}_n C_{n-1} 2^{n-n+1} + {}_n C_n 2^{n-n} \\
 4^n &= (3+1)^n = {}_n C_0 3^n + {}_n C_1 3^{n-1} + {}_n C_2 3^{n-2} + \cdots + {}_n C_{n-1} 3^{n-n+1} + {}_n C_n 3^{n-n} \\
 5^n &= (4+1)^n = {}_n C_0 4^n + {}_n C_1 4^{n-1} + {}_n C_2 4^{n-2} + \cdots + {}_n C_{n-1} 4^{n-n+1} + {}_n C_n 4^{n-n} \\
 +)6^n &= (5+1)^n = {}_n C_0 5^n + {}_n C_1 5^{n-1} + {}_n C_2 5^{n-2} + \cdots + {}_n C_{n-1} 5^{n-n+1} + {}_n C_n 5^{n-n}
 \end{aligned}$$

これは、

$$\begin{aligned}
 2^n &= (1+1)^n = 1^n + {}_n C_1 1^{n-1} + {}_n C_2 1^{n-2} + \cdots + {}_n C_{n-1} 1^{n-n+1} + {}_n C_n 1^{n-n} \\
 3^n &= (2+1)^n = 2^n + {}_n C_1 2^{n-1} + {}_n C_2 2^{n-2} + \cdots + {}_n C_{n-1} 2^{n-n+1} + {}_n C_n 2^{n-n} \\
 4^n &= (3+1)^n = 3^n + {}_n C_1 3^{n-1} + {}_n C_2 3^{n-2} + \cdots + {}_n C_{n-1} 3^{n-n+1} + {}_n C_n 3^{n-n} \\
 5^n &= (4+1)^n = 4^n + {}_n C_1 4^{n-1} + {}_n C_2 4^{n-2} + \cdots + {}_n C_{n-1} 4^{n-n+1} + {}_n C_n 4^{n-n} \\
 +)6^n &= (5+1)^n = 5^n + {}_n C_1 5^{n-1} + {}_n C_2 5^{n-2} + \cdots + {}_n C_{n-1} 5^{n-n+1} + {}_n C_n 5^{n-n}
 \end{aligned}$$

となるので、移項して、

$$\begin{aligned}
 2^n - 1^n &= {}_n C_1 1^{n-1} + {}_n C_2 1^{n-2} + \cdots + {}_n C_{n-1} 1^{n-n+1} + {}_n C_n 1^{n-n} \\
 3^n - 2^n &= {}_n C_1 2^{n-1} + {}_n C_2 2^{n-2} + \cdots + {}_n C_{n-1} 2^{n-n+1} + {}_n C_n 2^{n-n} \\
 4^n - 3^n &= {}_n C_1 3^{n-1} + {}_n C_2 3^{n-2} + \cdots + {}_n C_{n-1} 3^{n-n+1} + {}_n C_n 3^{n-n} \\
 5^n - 4^n &= {}_n C_1 4^{n-1} + {}_n C_2 4^{n-2} + \cdots + {}_n C_{n-1} 4^{n-n+1} + {}_n C_n 4^{n-n} \\
 +)6^n - 5^n &= {}_n C_1 5^{n-1} + {}_n C_2 5^{n-2} + \cdots + {}_n C_{n-1} 5^{n-n+1} + {}_n C_n 5^{n-n} \\
 6^n - 1^n &= {}_n C_1 \{1^{n-1} + 2^{n-1} + 3^{n-1} + 4^{n-1} + 5^{n-1}\} \\
 &\quad + {}_n C_2 \{1^{n-2} + 2^{n-2} + 3^{n-2} + 4^{n-2} + 5^{n-2}\} \\
 &\quad + {}_n C_3 \{1^{n-3} + 2^{n-3} + 3^{n-3} + 4^{n-3} + 5^{n-3}\} \\
 &\quad + {}_n C_4 \{1^{n-4} + 2^{n-4} + 3^{n-4} + 4^{n-4} + 5^{n-4}\} \\
 &\quad + {}_n C_5 \{1^{n-5} + 2^{n-5} + 3^{n-5} + 4^{n-5} + 5^{n-5}\} \\
 &\quad + \qquad \qquad \qquad \cdot \\
 &\quad + {}_n C_r \{1^{n-r} + 2^{n-r} + 3^{n-r} + 4^{n-r} + 5^{n-r}\} \\
 &\quad + \qquad \qquad \qquad \cdot \\
 &\quad + {}_n C_n \{1^{n-n} + 2^{n-n} + 3^{n-n} + 4^{n-n} + 5^{n-n}\}
 \end{aligned}$$

そこで、

$$\begin{aligned}
6^n - 1^n = & {}_n C_1 \{1^{n-1} + 2^{n-1} + 3^{n-1} + 4^{n-1} + 5^{n-1}\} \\
& + {}_n C_2 \{1^{n-2} + 2^{n-2} + 3^{n-2} + 4^{n-2} + 5^{n-2}\} \\
& + {}_n C_3 \{1^{n-3} + 2^{n-3} + 3^{n-3} + 4^{n-3} + 5^{n-3}\} \\
& + {}_n C_4 \{1^{n-4} + 2^{n-4} + 3^{n-4} + 4^{n-4} + 5^{n-4}\} \\
& + {}_n C_5 \{1^{n-5} + 2^{n-5} + 3^{n-5} + 4^{n-5} + 5^{n-5}\} \\
& + \quad \cdot \\
& + {}_n C_r \{1^{n-r} + 2^{n-r} + 3^{n-r} + 4^{n-r} + 5^{n-r}\} \\
& + \quad \cdot
\end{aligned}$$

また、

$$+ {}_n C_n \{1^{n-n} + 2^{n-n} + 3^{n-n} + 4^{n-n} + 5^{n-n}\}$$

は、

$$+ \{1^0 + 2^0 + 3^0 + 4^0 + 5^0\}$$

であり、

$$+ (6 - 1)\}$$

となる。ところで、 ${}_n C_r$ において、 n が素数ならば、 ${}_n C_r$ は n の倍数であるから、

$$6^n - 1^n = nP(6) + 6 - 1 \quad \text{ただし、} nP(6) = {}_n C_1 \{\dots\} + {}_n C_2 \{\dots\} + \dots + {}_n C_{n-1} \{\dots\} \text{である。}$$

よって、

$$6^n = nP(6) + 6$$

一般に、

$$\begin{aligned}
a^n - 1^n = & {}_n C_1 \{1^{n-1} + 2^{n-1} + 3^{n-1} + 4^{n-1} + \dots + (a-1)^{n-1}\} \\
& + {}_n C_2 \{1^{n-2} + 2^{n-2} + 3^{n-2} + 4^{n-2} + \dots + (a-1)^{n-2}\} \\
& + {}_n C_3 \{1^{n-3} + 2^{n-3} + 3^{n-3} + 4^{n-3} + \dots + (a-1)^{n-3}\} \\
& + {}_n C_4 \{1^{n-4} + 2^{n-4} + 3^{n-4} + 4^{n-4} + \dots + (a-1)^{n-4}\} \\
& + {}_n C_5 \{1^{n-5} + 2^{n-5} + 3^{n-5} + 4^{n-5} + \dots + (a-1)^{n-5}\} \\
& + \quad \cdot \\
& + {}_n C_r \{1^{n-r} + 2^{n-r} + 3^{n-r} + 4^{n-r} + \dots + (a-1)^{n-r}\} \\
& + \quad \cdot
\end{aligned}$$

また、

$$+ {}_n C_n \{1^{n-n} + 2^{n-n} + 3^{n-n} + 4^{n-n} + \dots + (a-1)^{n-n}\}$$

は、

$$+ \{1^0 + 2^0 + 3^0 + 4^0 + \dots + (a-1)^0\}$$

であり、

$$+ (a - 1)\}$$

となる。ところで、 ${}_nC_r$ において、 n が素数ならば、 ${}_nC_r$ は n の倍数であるから、

$$a^n = nA + a \text{ ただし、} nA = {}_nC_1\{\dots\} + {}_nC_2\{\dots\} + \dots + {}_nC_{n-1}\{\dots\} \text{ である。}$$

1.3 フェルマーの小定理

ここで、

$$a^n = nA + a$$

$$a^n - a = nA$$

$$a(a^{n-1} - 1) = nA$$

$$a^{n-1} - 1 \equiv 0 \pmod{n} \quad a \text{ と } n \text{ は互いに素とすると両辺を } a \text{ で割れる}$$

$$a^{n-1} \equiv 1 \pmod{n} \text{ ただし、} n \text{ は素数で } a \text{ と } n \text{ は互いに素}$$

よって、フェルマーの小定理が証明された。