

FermatLittleTheorem

Katabami

2025 年 6 月 23 日

Theorem 1 (Fermat's Little theorem). p を素数とする。このとき p と互いに素である自然数 n に対して、以下の合同式が成り立つ

$$n^{p-1} \equiv 1 \pmod{p}$$

このことを、1 から $p-1$ を p で割った余りを用いて証明する。

Proof. まず、 $n, 2n, \dots, (p-1)n$ を p で割った余りがどの 2 つも相異なることを示す。

任意の $i, j \in \mathbb{N}$ ($0 < i \leq j < p$) に対して $jn - in = (j-i)n$ を p で割った余りが 0 となる必要十分条件を考える。

いま、 p は素数かつ n と互いに素であり、 $0 < j-i < p$ なので、 $(j-i)n \equiv 0 \pmod{p}$ となる場合は必ず $i = j$ である。したがって、 $n, 2n, \dots, (p-1)n$ を p で割った余りはすべて異なる。

よって、

$$n \cdot 2n \cdot \dots \cdot (p-1)n \equiv 1 \cdot 2 \cdot \dots \cdot (p-1) \pmod{p}$$

すなわち、

$$n^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

$(p-1)!$ は p と互いに素であるため、両辺を $(p-1)!$ で割ることで

$$n^{p-1} \equiv 1 \pmod{p}$$

□

Theorem 2 (Fermat's Little theorem). 同様の定理を、二項定理による展開を用いた帰納法により証明する。

Proof.

$$1^p \equiv 1 \pmod{p}$$

は明らかである。ここで、

$$n^p \equiv n \pmod{p}$$

という仮定のもとで、

$$(n+1)^p \equiv n+1 \pmod{p}$$

を示す。

$$(n+1)^p = \sum_{k=0}^p \binom{p}{k} n^k \cdot 1^{p-k} = \sum_{k=1}^{p-1} \binom{p}{k} n^k + n + 1$$

ここで、 $1 \leq k \leq p-1$ のとき $\binom{p}{k}$ は p の倍数であるため、

$$\sum_{k=1}^{p-1} \binom{p}{k} n^k \equiv 0 \pmod{p}$$

ゆえに、

$$(n+1)^p \equiv n+1 \pmod{p}$$

したがって、数学的帰納法により $n^p \equiv n \pmod{p}$ が成り立つ。

ここで、 n と p が互いに素であるから、両辺を n で割って、

$$n^{p-1} \equiv 1 \pmod{p}$$

□

Theorem 3. 最後に、ラグランジュの定理を用いた証明を行う。

Proof. ラグランジュの定理とは、有限群 G とその部分群 H に対して、

(1) $|G| = (G : H)|H|$

(2) 任意の $g \in G$ の位数は $|G|$ の約数である

という性質が成り立つという定理である。

これを用いてフェルマーの小定理を証明する。

有限体 $\mathbb{Z}/p\mathbb{Z}$ の乗法群 $(\mathbb{Z}/p\mathbb{Z})^\times$ の位数は $p-1$ である。

ラグランジュの定理より、 $n \in (\mathbb{Z}/p\mathbb{Z})^\times$ の位数を d とすると、これは $p-1$ の約数なので $p-1 = dm$ ($m \in \mathbb{N}$) と書ける。

したがって、

$$n^{p-1} = n^{dm} = (n^d)^m \equiv 1^m = 1 \pmod{p}$$

である。

□