

素数の無限性

ナンブ キトラ

2026年7月17日

この文章では素数の無限性を証明する.

定義 1. $n, m \in \mathbb{Z}_{\geq 1}$ とする. $n = km$ となる $k \in \mathbb{Z}_{\geq 1}$ が存在するときに m は n の約数という. $p \in \mathbb{Z}_{\geq 1}$ が素数であるとは $p \neq 1$ であり尚且つ p が 1 と自分自身以外の正の約数を持たないときにいう. n の素因数とは素数であり n を割り切れる数のことである. そして $n \in \mathbb{Z}_{\geq 1}$ に対して $1 < a, b < n$ を満たす $a, b \in \mathbb{Z}_{\geq 1}$ が存在して $n = ab$ を満たすならば n を合成数と呼ぶ.

合成数の定義から次がわかる.

命題 2. n が合成数であることと $n \neq 1$ で尚且つ n が素数でないことは同値である.

命題 3. $n \in \mathbb{Z}_{\geq 1}$ が $n \neq 1$ を満たすならば n は素因数を持つ.

証明. まず $A = \{n \in \mathbb{N} \mid n \neq 1 \text{ かつ } n \text{ は素因数を持たない}\}$ とおく. 命題は $A = \emptyset$ と同値である. 今 $A \neq \emptyset$ と仮定すると A の最小元が存在する. $a = \min A$ と置く. $a \in A$ なので $a \neq 1$ であり, a は素数ではない. よって命題 2 より a は合成数である. ゆえに $a = xy$ ($1 < x, y < a$) と書ける. a の最小性から $x, y \notin A$ である. よって x, y は素因数を持つことから a も素因数を持つことになり矛盾する. $\square$

定理 4. 素数は無限に存在する.

証明. 任意の $n > 1$ に対してそれよりも大きい素数が存在するを言えば良い. $n!$ を 1 から n までの間の自然数の積とする. このとき $n! + 1$ は命題 3 より素因数を持つ. その素因数の一つを p とする. $(n! + 1) - n! = 1$ なので, もしも p が $n!$ の約数だとすると p は 1 を割り切ることになり $p = 1$ となる. これは p が素数であることに矛盾する. よって p は $n!$ の約数ではないので, $n!$ の定義から $n < p$ である. $\square$