素因数分解の一意性の直接的証明

定義 1　正の整数 p が**素数**であるとは, 次の 2 条件をみたすことをいう:

(i) $p \neq 1$.
(ii) 任意の正の整数 a, b に対して,

$$p = ab \Longrightarrow a = 1 \text{ または } a = p$$

が成り立つ.

例 1　2 は素数である. 実際, a, b を正の整数とし, $2 = ab$ であるとすると, $a \leq 2$ かつ $b \leq 2$ である. よって,

$$(a, b) = (1, 1), (1, 2), (2, 1), (2, 2)$$

の 4 通りが考えられるが, そのうち

$$(a, b) = (1, 2), (2, 1)$$

のみが $2 = ab$ を満たす. したがって, $a = 1$ または $a = 2$ である.

定理 1　1 以外の正の整数はすべて素数の積の形で表せる.

証明　n に関する数学的帰納法により証明する.

2 は素数であるから, $n = 2$ のとき定理の主張は正しい.

$2 \leq k \leq n-1$ なるすべての整数 k に対して定理の主張が正しいと仮定する. n が素数のとき, 定理の主張が正しいことは自明である. n が素数でな

いとき, ある正の整数 a, b が存在して,

$$n = ab, \quad 1 < a < n, \quad 1 < b < n$$

が成り立つ. 帰納法の仮定により, a, b はともに素数の積の形で表せる. したがって, n も素数の積の形で表せる.

以上より, すべての整数 $n \geq 2$ に対して定理の主張が正しいことが証明された. □

定義 2 n を正の整数とする. n の約数であるような素数を n の**素因数**という.

定義 3 正の整数を素数の積の形で表すことを**素因数分解**という.

定理 1 は「1 以外の正の整数はすべて素因数分解が可能である」と言いかえることができる.

補題 2 p, q_1, q_2, …, q_t を素数とする. このとき,

$$p = q_1 q_2 \cdots q_t$$

ならば, $t = 1$ かつ $p = q_1$ が成り立つ.

証明 背理法により証明する. もし仮に $t > 1$ とすると, $q_1 = 1$ または $q_1 = p$ が成り立つ. $q_1 \neq 1$ であるから, $q_1 = p$. よって, $q_2 \cdots q_t = 1$. これは矛盾である. したがって, $t = 1$ でなければならない. またこのとき,

$p = q_1$ となる. □

定理 3　素因数分解は, 素因数の積の順序を除いて一意的である.

証明　n に関する数学的帰納法により証明する.

2 は素数であるから, 補題 2 より 2 の素因数分解は一意的である. よって, $n = 2$ のとき定理の主張は正しい.

$2 \leq k \leq n-1$ なるすべての整数 k について素因数分解の一意性が成り立つと仮定する. n が素数の場合, 補題 2 より n の素因数分解は一意的である. n が素数でない場合, n の素因数分解が

$$n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$$

のように 2 通りあるとする. 今は n が素数でない場合を考えているので, $s \geq 2$ かつ $t \geq 2$ であることを注意しておく.

番号を適当に付けかえて,

$$p_1 \leq p_2 \leq \cdots \leq p_s, \quad q_1 \leq q_2 \leq \ldots \leq q_t \tag{1}$$

としておく.

まず, $p_1 = q_1$ が成り立つことを背理法により証明する. $q_1 < p_1$ が成り立つと仮定して矛盾を導く[1)]. 背理法の仮定と (1) より

$$q_1 < p_i \quad (i = 1, 2, \ldots, s) \tag{2}$$

が成り立つ.

$$m = (p_1 - q_1) p_2 \cdots p_s \tag{3}$$

[1)] $p_1 < q_1$ のときも同様にして矛盾が導かれる.

とおくと, $0 < p_1 - q_1 < p_1$ であるから, m は n より小さい正の整数である. 帰納法の仮定により, m の素因数分解は一意的である. さらに,

$$\begin{aligned} m &= (p_1 - q_1)p_2 \cdots p_s \\ &= n - q_1 p_2 \cdots p_s \\ &= q_1(q_2 \cdots q_t - p_2 \cdots p_s). \end{aligned} \tag{4}$$

Case 1 $q_2 \cdots q_t - p_2 \cdots p_s > 1$ の場合, 定理 1 より

$$q_2 \cdots q_t - p_2 \cdots p_s = v_1 v_2 \cdots v_r$$

のように素因数分解することができる. これを (4) に代入すると

$$m = q_1 v_1 v_2 \cdots v_r \tag{5}$$

が得られる.

(Case 1-1) $p_1 - q_1 > 1$ の場合, 定理 1 より, $p_1 - q_1$ を

$$p_1 - q_1 = u_1 u_2 \cdots u_l$$

のように素因数分解することができる. これを (3) に代入すると,

$$m = u_1 u_2 \cdots u_l p_2 \cdots p_s.$$

これと (5) と m の素因数分解の一意性より, q_1 は $u_1, \ldots, u_l, p_2, \ldots, p_s$ のどれかと一致する. もし仮に $p_2, \ldots, p_s$ のどれかと一致すると (2) に反するから, q_1 は $u_1, \ldots, u_l$ のどれかと一致する. 例えば $q_1 = u_1$ とすると,

$$p_1 - q_1 = q_1 u_2 \cdots u_l.$$

両辺に q_1 を加えると,

$$p_1 = q_1(u_2 \cdots u_l + 1).$$

p_1 は素数だから, $q_1 = 1$ または $q_1 = p_1$. 前者は q_1 が素数であることに反し, 後者は (2) に反する.

(Case 1-2)　$p_1 - q_1 = 1$ の場合, (3) より

$$m = p_2 \cdots p_s.$$

これと (5) と m の素因数分解の一意性より, q_1 は p_2, ..., p_s のどれかと一致する. これは (2) に反する.

Case 2　$q_2 \cdots q_t - p_2 \cdots p_s = 1$ の場合, (4) より $m = q_1$ が得られる. さらに (3) より,

$$q_1 = (p_1 - q_1)p_2 \cdots p_s.$$

q_1 は素数だから, $p_1 - q_1 = 1$ または $p_1 - q_1 = q_1$. 前者の場合,

$$q_1 = p_2 \cdots p_s.$$

これと補題 2 より $q_1 = p_2$ となり, (2) と矛盾する. 後者の場合, $p_1 = 2q_1$ となるが, 2, p_1, q_1 はすべて素数だから, これは不可能である.

ゆえに, $p_1 = q_1$ でなければならない. またこのとき, $n/p_1 = n/q_1$, すなわち

$$\frac{n}{p_1} = p_2 \cdots p_s = q_2 \cdots q_t.$$

帰納法の仮定により n/p_1 について素因数分解の一意性が成り立つから, (1) と合わせれば $r = s$ かつ $p_i = q_i$ $(i = 2, \ldots, r)$ である. したがって, n についても素因数分解の一意性が成り立つ.

以上より, すべての整数 $n \geq 2$ に対して定理の主張が正しいことが証明された. □

補足説明

初等整数論の教科書では通常, 素因数分解の一意性を次の 2 つのステップで証明する:

Step 1 整数環 $\mathbb{Z}$ においては「既約元」がすべて「素元」になる (逆は一般に整域において成り立つ).

Step 2 1 以外の正の整数が「素元」の積の形で表されるならば, その表し方は一意的である.

今回紹介した証明では, Step 1 を飛ばして「既約元」の積の形での表し方が一意的であることを直接証明している.