第4章　素数と素因数分解の一意性

4.1　素数の定義

定義 4.1 整数 p が**素数**であるとは，$p>1$ であって，$1<d<p$ をみたす約数 d をもたないものである．

素数でも 1 でも -1 でもない整数を**合成数**という（$1,-1$ は**単数**とよばれるが，いまは忘れちゃってもいい）． 一般に，整数 $n\neq 0$ に対して，$1,-1,n,-n$ を n の**自明な約数**という． したがって，素数とは自明な約数しかもたない 1 より大きい整数のことである． この定義は，p の “約数” に注目して述べられているが，以下のように p の “倍数” を用いて素数を特徴づけることもできる．

命題 4.2 整数 p が素数であるためには次が成り立つことが必要十分である； $p>1$ であって，$a,b\in \boldsymbol{Z}$ に対してその積 ab が p の倍数ならば，a または b は p の倍数である．

証明　必要性　p が素数であるとする． いま，$p|ab$ を仮定する． a,p の最大公約数 d は p の正の約数だが，p が素数なので，$d=p$ または $d=1$ となる． $d=p$ のとき，a が p の倍数であることは明らかである． 一方，$d=1$ のときは，定理 2.6（または 3.5）より，$ax+py=1$ $(x,y\in \boldsymbol{Z})$ と表されるから，$b=abx+pby$ は p の倍数となる．
十分性　d を p の約数とすると，$p=cd$ $(c\in \boldsymbol{Z})$ と書ける． もちろん $p|cd$ だから，仮定より $p|c$ または $p|d$ である． $p|c$ ならば $pk=c$ $(k\in \boldsymbol{Z})$ と表されるから，$p=cd=pkd$，よって $kd=1$ より $d=\pm 1$ を得る． $p|d$ のときは，$pl=d$ $(l\in \boldsymbol{Z})$ と書け，$p=cd=cpl$，よって $cl=1$ だから $c=\pm 1$ すなわち $d=\pm p$ となる． 以上より，p は自明な約数しかもたないことが示されたから，p は素数である． □

さて，素数の定義から直接導かれる性質として，任意の自然数 $a>1$ が有限個の素数の積に書けることがあげられる． 実際，素数の積で書けない $a>1$ があったとすると，その様な最小の自然数が存在する（最小値原理）． それをあらためて a とすれば，a はもちろん素数でないから，素数の定義より $a=bc,\ 1<b,c<a$ をみたす $b,c\in \boldsymbol{N}$ がとれるが，a の最小性より b,c は素数の積で書けるので，その積 a も書けることになり矛盾する．

自然数 a を素数の積に表すことを a の**素因数分解**といい，積に現れる素数を a の**素因数**または**素因子**という（$a=1$ のときも 0 個の素因数をもつ分解と考えることにする）．そして，素因数分解の仕方は順序を考えなければ一通りであることもよく知っているはずである． そのこともあわせて，定理としてまとめておく．

定理 4.3 (初等数論の基本定理) 1 より大きい任意の自然数 a は素数 $p_1, \cdots, p_r$ の積

$$a = p_1 \cdots p_r$$

として表すことができ，順序を考えなければその表し方は一意的である． すなわち，二通りの素数の積

$$a = p_1 \cdots p_r = q_1 \cdots q_s$$

に表されたとすると，$r = s$ であって，さらに $q_1, \cdots, q_r$ の番号をうまくとり換えれば $p_1 = q_1, \cdots, p_r = q_r$ とできる． （より正確に書けば，$\{1, 2, \cdots, r\}$ 上の置換 σ で $p_i = q_{\sigma(i)}$ $(i = 1, \cdots, r)$ をみたすものが存在する.）

証明 素因数分解が可能であることはすでに示した． 後半の表し方の一意性を示すために，二通りの素数の積として書ける自然数が存在するとして矛盾を導く． そのような最小の自然数を a とし，$a = p_1 \cdots p_r = q_1 \cdots q_s$ を二通りの素数の積とする． p_1 が素数でかつ $p_1 | q_1 \cdots q_s$ なので，命題 4.2 を（何度か）使えば，$p_1 | q_j$ をみたす j がとれることがわかる． もし $j \neq 1$ だったら順序を入れ換えて $j = 1$，すなわち $p_1 | q_1$ であるとしてよい．ここでさらに q_1 が素数であることから $p_1 = q_1$ を得る． したがって，$p_2 \cdots p_r = q_2 \cdots q_s$ であって，仮定より，両辺の積の表し方は（順序を入れかえたとしても）同じにはならない． しかも，この積は a よりも小さいので，a の最小性に矛盾することになる． □

定理 4.3 の後半の主張はとくに**素因数分解の一意性**と呼ばれる． その証明の中で，命題 4.2 の形での素数の特徴づけが使われていることに注目したい（が，ここでは深入りしない）.

さて，定理において，p_i のうち同じものをまとめることで，

$$a = p_1^{e_1} \cdots p_r^{e_r} \qquad (p_1, \cdots, p_r \text{ は相異なる素数}, e_i \geq 1)$$

と表すことができる． さらに必要ならば，p_i が素因数でない場合でも $e_i = 0$ として積に含めることができる（このとき $p_i^{e_i} = 1$ に注意）． たとえば，$20 = 2^2 \cdot 5^1 = 2^2 \cdot 3^0 \cdot 5^1$. このような表し方も素因数分解とよぶことにする.

次の定理および系の証明は演習とする.

定理 4.4 自然数 a, b の素因数分解が

$$a = p_1^{e_1} \cdots p_r^{e_r}, \quad b = p_1^{f_1} \cdots p_r^{f_r} \qquad (p_1, \cdots, p_r \text{ は相異なる素数}, e_i, f_i \geq 0)$$

で与えられたとき，次が成り立つ.

(1) $a | b \iff e_i \leq f_i$ $(i = 1, \cdots, r)$.

(2) $d_i = \min(e_i, f_i)$ $(i = 1, \cdots, r)$ とおけば，$\gcd(a, b) = p_1^{d_1} \cdots p_r^{d_r}$.

(3) $g_i = \max(e_i, f_i)$ $(i = 1, \cdots, r)$ とおけば，$\mathrm{lcm}(a, b) = p_1^{g_1} \cdots p_r^{g_r}$.

系 4.5 自然数 a, b に対して $d = \gcd(a, b),\ m = \mathrm{lcm}(a, b)$ とすると，$ab = dm$ が成り立つ．

p を素数とする． 自然数 a に対して，$p^e | a$ であるが $p^{e+1} \nmid a$ であるような整数 $e \geq 0$ がとれる． この e を $v_p(a)$ で表すと，a の素因数分解は

$$a = \prod_{p:\text{素数}} p^{v_p(a)}$$

と表すことができる． $v_p(-a) = v_p(a),\ v_p(0) = \infty$ と定めることで，v_p を $\boldsymbol{Z}$ 上の関数とみなすことができる (ただし，値として ∞ も許す)． この関数 v_p を p **進付値**という．

4.2 素数が無限個あること

次の定理は当たり前のようであるが，定理 4.3 との関連を考えると重要である．

定理 4.6 素数は無数に存在する．

以下において 2 通りの証明を与える（時間が許せば，講義でさらに別の証明も紹介する)． ひとつはユークリッドによる証明であり古代からよく知られていた方法，もうひとつは，オイラーによる示唆に富んだ方法である．

証明 [ユークリッド](古代) 素数が有限個しかないとして矛盾を導く． すべての素数を $p_1, \cdots, p_r$ とし，$M = p_1 \cdots p_r + 1$ とおく． 定理 4.3 より，M はある素数で割り切れる．仮定よりその素数は $p_1, \cdots, p_r$ のどれかである． それを p_i とすると，$1 = M - p_1 \cdots p_r$ が素数 p_i の倍数となって矛盾する． □

証明 [オイラー](18 世紀) ここでも，素数は有限個しかなく，それらすべてが $p_1, \cdots, p_r$ であるとして矛盾を導くことにする． いま，等比数列の和の公式より，各素数 $p = p_i$ について

$$\sum_{m=0}^{\infty} \frac{1}{p^m} = \frac{1}{1 - \frac{1}{p}} = \frac{p}{p-1}$$

であり，これらの積をとれば

$$(\spadesuit) \quad \frac{p_1}{p_1 - 1} \cdots \frac{p_r}{p_r - 1} = \left(\sum_{m_1=0}^{\infty} \frac{1}{p_1^{m_1}} \right) \cdots \left(\sum_{m_r=0}^{\infty} \frac{1}{p_r^{m_r}} \right) = \sum_{m_1=0}^{\infty} \cdots \sum_{m_r=0}^{\infty} \frac{1}{p_1^{m_1} \cdots p_r^{m_r}}.$$

あとの等式が正当化される理由は，絶対収束級数においては，和の順序をかってに換えたり，分配法則を自由に使って良いという性質があるからである（「微分積分」で教わったことを思い出そう ... もし忘れちゃってたら微積の単位没収だぞ！)． ここで，$p_1, \cdots, p_r$ がすべての素数であることから，定理 4.3 より，任意の自然数は

$$p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r} \qquad (m_1, m_2, \cdots, m_r \geq 0)$$

の形に一通りに表されている． よって，(♠) の最右辺はすべての自然数の逆数和であり

$$\frac{p_1 \cdots p_r}{(p_1-1)\cdots(p_r-1)} = \sum_{n=1}^{\infty} \frac{1}{n}$$

となるが，右辺は収束しない（これも微積でやったはず）から矛盾である． □

4.3 ゼータ関数

オイラーは，自然数 n の代わりにベキ数 n^s の逆数和を考え，無限級数

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots$$

が $s > 1$ のとき収束することに注目し，上の証明の手法を用いて，公式

$$\zeta(s) = \prod_{p} \frac{1}{1-p^{-s}} \qquad (s > 1)$$

を導いた． ここで，右辺は素数全体をわたる積でオイラー積と呼ばれている． さらに，s が正の偶数のときの $\zeta(s)$ の値

$$\zeta(2) = \frac{\pi^2}{6}, \qquad \zeta(4) = \frac{\pi^4}{90}, \qquad \zeta(6) = \frac{\pi^6}{945} \quad \text{など} \ldots$$

を得ている (1730 年代)． ここに円周率 π が現れるのは，なんとも不思議である． その後，リーマンは s の動く範囲を複素数にまで広げ，複素関数としての $\zeta(s)$（これを**ゼータ関数**という）の性質を調べている． その目的はガウスが予想した**素数定理**の証明であったが，研究途上で有名な予想を提唱した (1859 年)．

予想 4.7 (リーマン予想 (Riemann Hypothesis)) $\zeta(s) = 0$ をみたす実部が正の複素数 s はすべて $s = \dfrac{1}{2} + it$ (t は実数) の形をしているであろう．

リーマン予想は 150 年以上経過した現在でも未解決の問題として残っている． なお，素数定理そのものはリーマン予想がなくても証明できることが知られている．

定理 4.8 (素数定理) 正の実数 x に対して，x 以下の素数の個数を $\pi(x)$ とすると，

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1.$$

すなわち，十分大きな x について $\pi(x)$ は $\dfrac{x}{\log x}$ で近似される． 証明は，アダマールとド・ラ・ヴァレー・プーサンが独立に与えた (1896 年)． その方法は複素関数論（複素数上の微積分学）によるものだが，証明を書き下すだけの余白が，ここにもやっぱ無い．