第4章　素数

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．

一般に，整数 $n \neq 0$ に対して，± 1, $\pm n$ 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” を用いて述べられたが，以下のように “p の倍数” を通して素数を特徴づけることもできる．

命題 4.2 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，$p \mid ab$ を仮定する．a, p の最大公約数 d はもちろん p の正の約数なので，p が素数ということより，$d = p$ または $d = 1$ であることがわかる．$d = p$ のとき，$p \mid a$ である．一方，$d = 1$ のときは，定理 2.5（または 3.4）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　　$d > 0$ を p の約数とすると，$p = cd$ $(c \in \boldsymbol{Z})$ と書ける．もちろん $p \mid cd$ だから，仮定より $p \mid c$ または $p \mid d$ である．$p \mid c$ 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 $d = 1$ を得る．$p \mid d$ のときは，$pl = d$ $(l \in \boldsymbol{Z})$ と書け，$p = cd = cpl$，よって $cl = 1$ だから $c = 1$ すなわち $d = p$ となる．以上より，p の正の約数は $1, p$ しかないことが示されたから，p は素数である．　□

定理 4.3 (初等数論の基本定理) 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．）

2012 年度「代数入門」講義資料（2012 年 10 月）ver.1017

証明　素数の積に表せること:　まず，$a=1$ のときは $r=0$，つまり 0 個の素数の積で表されると考えればよい．以下，素数の積でかけない 1 より大きい自然数が存在するとして矛盾を導こう．最小値原理によって，そのような最小の自然数 a がとれる．a はもちろん素数ではないから，$a=bc$，$1<b,c<a$ となる $b,c\in\boldsymbol{N}$ が存在する．このとき，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．
表し方の一意性:　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．$p_1\mid q_1\cdots q_s$ なので，命題 4.2 を（何度か）使えば，$p_1\mid q_j$ をみたす j がとれることがわかる．順序を入れ換えて $j=1$ すなわち $p_1\mid q_1$ であるとしてよい．ここで，$p_1>1$ でありかつ 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同じではない．しかし，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．□

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．上の定理において，p_i のうち同じものをまとめることで，

$$a=p_1^{e_1}\cdots p_r^{e_r}\qquad (p_1,\cdots,p_r \text{ は相異なる素数，} e_i>0)$$

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

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

で与えられるとき次が成り立つ．

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

(2) $g_i=\min(e_i,f_i)\ (i=1,\cdots,r)$ とおけば，$\gcd(a,b)=p_1^{g_1}\cdots p_r^{g_r}$．

(3) $h_i=\max(e_i,f_i)\ (i=1,\cdots,r)$ とおけば，$\mathrm{lcm}(a,b)=p_1^{h_1}\cdots p_r^{h_r}$．

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

この系から，さらに，任意の $a,b\in\boldsymbol{Z}$ に対して $|ab|=\gcd(a,b)\,\mathrm{lcm}(a,b)$ がわかる（各自確かめてみよ）．

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．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) 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が，素数は $p_1, \cdots, p_r$ のどれかだから，それを p_i とする． このとき，$1 = M - p_1 \cdots p_r$ が素数 p_i の倍数となって矛盾である． □

オイラーによる証明の準備として次のようなことを考える． 2 と 3 以外に素因数をもたない自然数全体の逆数和を A とする． 分母の小さい順に並べれば，

$$A = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{6} + \frac{1}{8} + \frac{1}{9} + \frac{1}{12} + \frac{1}{16} + \frac{1}{18} + \frac{1}{24} + \frac{1}{27} + \frac{1}{32} + \cdots.$$

これを眺めても何だかよくわからないが，分母は $2^m 3^n$ の形をしているから，

$$A = \sum_{m,n=0}^{\infty} \frac{1}{2^m 3^n} = \sum_{m=0}^{\infty} \left(\sum_{n=0}^{\infty} \frac{1}{2^m 3^n} \right) = \left(\sum_{m=0}^{\infty} \frac{1}{2^m} \right) \left(\sum_{n=0}^{\infty} \frac{1}{3^n} \right)$$

と変形できるであろう． ここで，等比級数に関する公式を用いれば

$$\sum_{m=0}^{\infty} \frac{1}{2^m} = \frac{1}{1 - \frac{1}{2}} = 2, \qquad \sum_{n=0}^{\infty} \frac{1}{3^n} = \frac{1}{1 - \frac{1}{3}} = \frac{3}{2}$$

なので，はじめに与えた無限級数 A は確かに収束してその値は $2 \cdot \frac{3}{2} = 3$ となることがわかる（絶対収束級数においては，項の順序をかってに換えたり，分配法則を自由に使っていいよと１年生の微積で教わったはず）．

以上の考察をふまえてオイラーによる定理 4.6 の証明を紹介する．

証明 (オイラー) 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，各 $i = 1, \cdots, r$ について

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

であるが，これらの積をとれば

$$(\star) \qquad \sum_{m_1=0}^{\infty} \cdots \sum_{m_r=0}^{\infty} \frac{1}{p_1^{m_1} \cdots p_r^{m_r}} = \frac{p_1 \cdots p_r}{(p_1 - 1) \cdots (p_r - 1)}.$$

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

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

の形をしていることがいえる．よって，($\star$) の左辺はすべての自然数の逆数和であり

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

となるが，左辺は収束しないから矛盾である．□

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

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

を得ている．ここで，右辺の p は素数全体をわたる積である．さらに，

$$\zeta(2) = \frac{\pi^2}{6}, \qquad \zeta(4) = \frac{\pi^4}{90}$$

など，偶数 $2k$ に対する $\zeta(2k)$ の値を得ている (1730 年代)．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**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) $\zeta(s) = 0$ 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が，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) が，複素関数論（複素数上の微積分学）によるものでありここでは紹介しない．