第8章　既約剰余類群とオイラー関数

8.1　既約剰余類群

m を 2 以上の整数とし，α を法 m に関する剰余類，すなわち $\alpha \in \boldsymbol{Z}/m\boldsymbol{Z}$ とする． いま，$a \in \alpha$ とすると $\alpha = a + m\boldsymbol{Z}$ である． a が法 m に関して可逆ならば，α に属するすべての整数は法 m に関して可逆となる． さらに，整数 b が m を法とする a の逆元ならば，剰余類 $b + m\boldsymbol{Z}$ に属するすべての整数は法 m に関する a の逆元である． 一方，a が法 m に関する零因子ならば，α に属するすべての整数は法 m に関する零因子である（これらのことを確かめてみよ）． したがって，法 m に関する “可逆”，“逆元”，“零因子” という概念は，どれも法 m に関する剰余類がもっている性質ととらえることができる． 次の定義は，このような考え方によって与えられたものである．

定義 8.1 m を 2 以上の整数とし，$\alpha \in \boldsymbol{Z}/m\boldsymbol{Z}$ を剰余類とする．整数 a は $\alpha = a + m\boldsymbol{Z}$ をみたすとする．

(1)　a が法 m に関して可逆であるとき，α は**可逆**であるという．

(2)　整数 b が法 m に関する a の逆元であるとき，b の属する剰余類を α の**逆元**とよぶ．

(3)　a が法 m に関する零因子であるとき，α は**零因子**であるという．

剰余類の逆元は，もし存在するならば一意的である． 実際，β, γ がともに α の逆元であるとすると，$\alpha\beta = \alpha\gamma = \overline{1}$ だから，

$$\gamma = \overline{1}\gamma = (\alpha\beta)\gamma = (\beta\alpha)\gamma = \beta(\alpha\gamma) = \beta\overline{1} = \beta.$$

そこで，剰余類 α の逆元を α^{-1} で表す（場合によっては $1/\alpha$ と書くこともある）． たとえば，$7 \cdot 13 = 91 \equiv 1 \pmod{15}$ なので，$\boldsymbol{Z}/15\boldsymbol{Z}$ において $\overline{7}, \overline{13}$ はともに可逆であり互いに逆元，したがって $\overline{7}^{-1} = \overline{13}$ とか $\overline{13}^{-1} = \overline{7}$ と書くこともできる．

定義 8.2 m を 2 以上の整数とする． $\boldsymbol{Z}/m\boldsymbol{Z}$ に属する可逆な剰余類全体からなる集合を，**法 m に関する既約剰余類群**といい $(\boldsymbol{Z}/m\boldsymbol{Z})^\times$ で表す;

$$(\boldsymbol{Z}/m\boldsymbol{Z})^\times = \{\, \alpha \in \boldsymbol{Z}/m\boldsymbol{Z} \mid \alpha \text{ は可逆} \,\}.$$

この元を，**法 m に関する既約剰余類**ということがある．

定理 5.9 によって，次のように表わすこともできる．

$$\begin{aligned}(\boldsymbol{Z}/m\boldsymbol{Z})^{\times} &= \{\, a+m\boldsymbol{Z} \mid a\in\boldsymbol{Z},\ \gcd(a,m)=1 \,\}\\ &= \{\, a+m\boldsymbol{Z} \mid a\in\boldsymbol{Z},\ a \text{ は } m \text{ を法として可逆} \,\}\\ &= \{\, a+m\boldsymbol{Z} \mid a\in\boldsymbol{Z},\ a \text{ は } m \text{ を法として零因子でない} \,\}.\end{aligned}$$

さらに，それぞれの $a\in\boldsymbol{Z}$ は $1\le a<m$ の範囲に限定してもよい（どうしてかな？）．

例 8.3 $\boldsymbol{Z}/10\boldsymbol{Z}=\{\overline{0},\overline{1},\overline{2},\cdots,\overline{9}\}$ のうち，可逆な剰余類は $\overline{1},\overline{3},\overline{7},\overline{9}$ であり，零因子は $\overline{0},\overline{2},\overline{4},\overline{5},\overline{6},\overline{8}$ である（確かめ〜）． とくに，既約剰余類群は $(\boldsymbol{Z}/10\boldsymbol{Z})^{\times}=\{\overline{1},\overline{3},\overline{7},\overline{9}\}$ となる． ここで，$\overline{1},\overline{3},\overline{7},\overline{9}$ のそれぞれの逆元が何かは……，計算してみ．

法 m に関する既約剰余類群 $(\boldsymbol{Z}/m\boldsymbol{Z})^{\times}$ は,『積について閉じていて，各元の逆元がその中でとれる』という性質をもっている． これらの性質は $(\boldsymbol{Z}/m\boldsymbol{Z})^{\times}$ が乗法に関して “群” であることを示しているのだが，詳しくは「代数 I」をお楽しみに．

8.2 オイラー関数

定義 8.4 自然数 m に対して，$0\le a<m$ である整数 a のうち m と互いに素なものの個数を $\varphi(m)$ で表す． また，このようにして定まる自然数上の関数 φ を**オイラー関数**という．

すなわち，

$$\varphi(m)=\left|\{\, a\in\boldsymbol{Z} \mid 0\le a<m,\ \gcd(a,m)=1 \,\}\right|.$$

$m\ge 2$ のときは，法 m に関する既約剰余類の個数が $\varphi(m)$ に他ならない;

$$\varphi(m)=\left|(\boldsymbol{Z}/m\boldsymbol{Z})^{\times}\right|.$$

たとえば，$m=10$ のとき，$(\boldsymbol{Z}/10\boldsymbol{Z})^{\times}=\{\overline{1},\overline{3},\overline{7},\overline{9}\}$ だから $\varphi(10)=4$． 小さい m に対するオイラー関数の値は次の表のようになる (1 個間違いがある，どれでしょう？ もぉ，先生のいじわるぅ)．

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$\varphi(m)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	10	16	6	18

この表からも見えるように，オイラー関数の値は非常に不規則だが，次節で示す定理 8.6 の公式を用いれば，次のような不等式を導くことができる．

命題 8.5 自然数 $m\ge 2$ に対して，$\dfrac{m}{1+\log_2 m}\le\varphi(m)\le m-1.$

この命題から，$\varphi(m)\to\infty$ $(m\to\infty)$ が導かれる． 右側の不等式は φ の定義から明らかだが，左側の証明は少し面倒である（補遺参照）．

8.3　オイラー関数の積公式

次の定理によって，どんなに大きな m についても，その素因数分解さえわかればオイラー関数の値 $\varphi(m)$ を正確に計算できる．

定理 8.6 自然数 m の素因数分解が $m=\prod_{j=1}^{r} p_j^{e_j}$ (p_j は相異る素数で $e_j>0$) ならば，

$$\varphi(m)=\prod_{j=1}^{r}\left(p_j^{e_j}-p_j^{e_j-1}\right)=m\prod_{j=1}^{r}\left(1-\frac{1}{p_j}\right).$$

たとえば，$126225=3^3\cdot 5^2\cdot 11\cdot 17$ だから

$$\varphi(126225)=(27-9)(25-5)(11-1)(17-1)=57600$$

と計算される． この定理は，以下の 2 つの補題から導くことがキミならできるはずだ．

補題 8.7 素数のべき p^e ($e>0$) に対して $\varphi(p^e)=p^e-p^{e-1}$.

証明　φ の定義を見れば，p^e と互いに素なもんの個数を数えればええやん． ある整数が p^e と互いに素っちゅうことは，そいつが p で割り切れないことと同じや． そやから，$\varphi(p^e)$ の値は，$0\le a<p^e$ をみたす整数 a 全部の個数 p^e から，p の倍数の個数を引けばええんとちゃう？ ほんでもって，p の倍数は $a=jp,\ 0\le j<p^{e-1}$ で表される p^{e-1} 個で全部やから，$\varphi(p^e)=p^e-p^{e-1}$ が答えっちゅうわけや． □

補題 8.8 互いに素な自然数 m,n に対して $\varphi(mn)=\varphi(m)\varphi(n)$.

証明　まず，m,n は互いに素な整数なので，前章，定理 7.6 より，写像

$$F\ :\ \boldsymbol{Z}/mn\boldsymbol{Z}\longrightarrow(\boldsymbol{Z}/m\boldsymbol{Z})\times(\boldsymbol{Z}/n\boldsymbol{Z}),\qquad a+mn\boldsymbol{Z}\mapsto(a+m\boldsymbol{Z},\,a+n\boldsymbol{Z})$$

は全単射であることに注意しておく． いま，整数 a が mn と互いに素ならば，a は m とも n とも互いに素になることは明らかである． したがって，F を既約剰余類群 $(\boldsymbol{Z}/mn\boldsymbol{Z})^\times$ に制限することにより，写像

$$G\ :\ (\boldsymbol{Z}/mn\boldsymbol{Z})^\times\longrightarrow(\boldsymbol{Z}/m\boldsymbol{Z})^\times\times(\boldsymbol{Z}/n\boldsymbol{Z})^\times$$

が定まる． F が単射なので G も単射であるが，以下において G は全射でもあることを確かめよう． これにより，元の個数を比べて $\varphi(mn)=\varphi(m)\varphi(n)$ となって証明が完了する． そこで，全射性を示すために，$\xi\in(\boldsymbol{Z}/m\boldsymbol{Z})^\times\times(\boldsymbol{Z}/n\boldsymbol{Z})^\times$ を任意にとって，

$$\xi=(a+m\boldsymbol{Z},\,b+n\boldsymbol{Z}),\qquad \gcd(a,m)=\gcd(b,n)=1$$

のように $a,b\in\boldsymbol{Z}$ で表せば，中国の剰余定理 (定理 6.5) より，

$$x\equiv a\pmod m,\qquad x\equiv b\pmod n$$

をみたす $x \in \boldsymbol{Z}$ が存在する（ここんとこ，F が全射であることを使ってもよい）． このとき，$\gcd(a,m) = \gcd(b,n) = 1$ から，$\gcd(x, mn) = 1$ が簡単に確かめられる． よって $x + mn\boldsymbol{Z} \in (\boldsymbol{Z}/mn\boldsymbol{Z})^{\times}$ かつ $G(x + mn\boldsymbol{Z}) = \xi$ であり，全射であることが示された． □

上の証明もそのアイデアの出所であった定理 7.6 の証明も，一見，同じことをやっているように見える． しかし，上の証明では，2 つの集合の間に単射があるときに，その写像の全射性から集合の元の個数が等しいことを導いているのに対し，定理 7.6 の証明では，逆に元の個数が等しいことから全射性を導いている． これらに違いに注目して二つの証明のストーリーを味わえるようになれば，キミも立派な数学科学生というわけだにゃん．

8.4 オイラー関数の和公式

自然数 m とその正の約数 d に対して，0 以上 m 未満の整数で，m との最大公約数が d であるもの全体の集合を $A(m,d)$ で表す;

$$A(m,d) = \{\, a \in \boldsymbol{Z} \mid 0 \le a < m,\ \gcd(a,m) = d \,\}.$$

とくに，$|A(m,1)| = \varphi(m)$，$|A(m,m)| = |\{0\}| = 1$ である． また，0 以上 m 未満の m 個の整数は m との最大公約数によって類別されるから，

$$\bigcup_{d|m} A(m,d) = \{0, 1, 2, \ldots, m-1\}$$

したがって

$$\sum_{d|m} |A(m,d)| = m$$

が成り立っている（m の正の約数 d 全体についての和をとる）．いま，$a \in A(m,d)$ に対して a/d は，集合

$$B = \left\{ b \in \boldsymbol{Z} \,\middle|\, 0 \le b < \frac{m}{d},\ \ \gcd\left(b, \frac{m}{d}\right) = 1 \right\}$$

に属する． すなわち，写像 $A(m,d) \to B,\ a \mapsto a/d$ が定義できるが，この写像が全単射であることを確かめるのは難しくない（実際，$B \to A(m,d),\ b \mapsto bd$ が逆写像となっている）． よって $|A(m,d)| = |B|$． 一方，φ の定義から B の元の個数は $\varphi(m/d)$ だから，$|A(m,d)| = \varphi(m/d)$ が導かれる． さらに，d が m の正の約数全体を動くとき m/d も正の約数全体を動くから，上の総和の式と合わせて次の定理を得る．

定理 8.9 自然数 m に対して，$\displaystyle\sum_{d|m} \varphi(d) = m.$

たとえば，$m = 15$ とすると，$\varphi(1) + \varphi(3) + \varphi(5) + \varphi(15) = 1 + 2 + 4 + 8 = 15$ となる．