既約剰余類と Euler 関数

m を自然数とする。$1, 2, \cdots, m$ の中で m と互いに素なものの個数を $\varphi(m)$ で表し，これを Euler 関数という。$1, 2, \cdots, m$ のうち m と互いに素なものを，$x_1, x_2, \cdots, x_{\varphi(m)}$ とするとき $\{x_1 \pmod m, x_2 \pmod m, \cdots, x_{\varphi(m)} \pmod m\}$ を $\bmod m$ の既約剰余類といい $(\mathbb{Z}/m\mathbb{Z})^*$ などと書く。

定理（Euler）

m を自然数，a を m と互いに素な整数とするとき

$$a^{\varphi(m)} \equiv 1 \pmod m$$

である。

$1, 2, \cdots, m$ のうち m と互いに素なものを，小さいものから順に

$$x_1, x_2, \cdots, x_{\varphi(m)}$$

とする。まず，$ax_1, ax_2, \cdots, ax_{\varphi(m)}$ は $\bmod m$ ですべて互いに異なることを示そう。仮に，$ax_i \equiv ax_j \pmod m$ $(i < j)$ とすると $a(x_j - x_i)$ は m の倍数となるが a と m は互いに素であるから $x_j - x_i$ が m の倍数でなければならない。しかし $0 < x_j - x_i < m$ であるからこれは不可能である。よって $ax_1, ax_2, \cdots, ax_{\varphi(m)}$ は $\bmod m$ ですべて互いに異なることが示された。

一方，a も x_i も m と互いに素であるから $ax_1, ax_2, \cdots, ax_{\varphi(m)}$ はすべて m と互いに素である。

従って，

$A = \{x_1 \pmod m, x_2 \pmod m, \cdots, x_{\varphi(m)} \pmod m\}$

も

$B = \{ax_1 \pmod m, ax_2 \pmod m, \cdots, ax_{\varphi(m)} \pmod m\}$

も，ともに $\bmod m$ での既約剰余類をなすので $\bmod m$ で考えるとき，A の要素の積と B の要素の積は一致する。よって

$$x_1x_2\cdots x_{\varphi(m)} \equiv ax_1ax_2\cdots ax_{\varphi(m)} \pmod m$$
$$x_1x_2\cdots x_{\varphi(m)} \equiv a^{\varphi(m)}x_1x_2\cdots x_{\varphi(m)} \pmod m$$
$$\left(a^{\varphi(m)} - 1\right)x_1x_2\cdots x_{\varphi(m)} \equiv 0 \pmod m$$

となる。従って $\left(a^{\varphi(m)} - 1\right)x_1x_2\cdots x_{\varphi(m)}$ は m の倍数であるが，$x_1x_2\cdots x_{\varphi(m)}$ は m と互いに素であるから $a^{\varphi(m)} - 1$ が m の倍数でなければならない。よって $a^{\varphi(m)} - 1 \equiv 0 \pmod m$ つまり $a^{\varphi(m)} \equiv 1 \pmod m$ である。■

［注］ Euler の定理において，特に $m = p$ を素数とすると，$\varphi(p) = p - 1$ であるから次を得る。

定理（Fermat の小定理）

p が素数のとき，a が p と素なら

$$a^{p-1} \equiv 1 \pmod{p}$$

$\varphi(m)$ の値を計算することを考える。

p を素数とするとき $1, 2, \cdots, p$ の中で p と互いに素なものは $1, 2, \cdots, p-1$ の $p-1$ 個であるから

p が素数のとき $\varphi(p) = p - 1$

である。

また，$m = p^e$ (p は素数，e は自然数) とするとき $1, 2, \cdots, p^e$ のうち p と互いに素でないのは p で割り切れるものに他ならないが，そのようなものは $1 \cdot p,\ 2 \cdot p,\ \cdots,\ p^{e-1} \cdot p$ の p^{e-1} 個あるから，p と互いに素なものは $p^e - p^{e-1}$ 個ある。よって

p が素数で e が自然数のとき $\varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$

である。

更に

m, と n が互いに素な自然数のとき $\varphi(mn) = \varphi(m)\varphi(n)$

となることを示そう。

$\{a_1 \pmod{m},\ a_2 \pmod{m},\ \cdots,\ a_{\varphi(m)} \pmod{m}\}$ を mod m の既約剰余類とし，

$\{b_1 \pmod{n},\ b_2 \pmod{n},\ \cdots,\ b_{\varphi(n)} \pmod{n}\}$ を mod n の既約剰余類とする。

また $1 \leqq i \leqq \varphi(m)$，$1 \leqq j \leqq \varphi(n)$ とする。

このとき 中国の剰余定理 によって $\begin{cases} x \equiv a_i \pmod{m} \\ x \equiv b_j \pmod{n} \end{cases}$ となる x が mod mn で考えてただひとつある。このとき x は m とも n とも互いに素であるから mn と互いに素となる。

逆に x を mn と互いに素な整数とすると x は m とも n とも互いに素であるから $x \equiv a_i \pmod{m}$，$x \equiv b_j \pmod{n}$ となる $a_i,\ b_j$ の組がひと組存在する。以上で $(a_i,\ b_j)$ という $\varphi(m)\varphi(n)$ 個の組と mod mn の既約剰余類が $1:1$ に対応することが分かったので $\varphi(mn) = \varphi(m)\varphi(n)$ となる。

［例］

(1) $\varphi(30) = \varphi(2)\varphi(3)\varphi(5) = (2-1)\cdot(3-1)\cdot(5-1) = 8$

(2) $\varphi(45) = \varphi(3^2)\varphi(5) = (3^2 - 3)\cdot(5-1) = 24$