オイラーの関数

1.　オイラーの関数の定義

オイラーの関数 $\varphi(n)$ は、自然数 n に対して、$1, 2, \ldots, n$ のうち、n と互いに素なものの個数を表す関数である。オイラーの関数の値は、n が小さければ、定義通りに調べることで求めることができる。例えば、$\varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2, \varphi(5) = 4, \varphi(6) = 2$ 等となる。

2.　オイラーの関数の値

一般に、オイラーの関数の値がどのようになるかを調べてみよう。まず、$n = p^e$ の場合を考えてみると、

$$\varphi(p^e) = p^e - p^{e-1} \tag{1}$$

であることがわかる。なぜなら、$1, 2, \ldots, p^e$ のうち、p^e と互いに素でないものは、p の倍数であるものだけであり、それらは、$p, 2p, \ldots, p^e$ の p^{e-1} 個であるからである。

次に、m と n が互いに素であるときに、

$$\varphi(mn) = \varphi(m)\varphi(n) \tag{2}$$

であることを示してみよう。

まず、$1, 2, \ldots, m$ のうち、m と互いに素な数を、$a_1, a_2, \ldots, a_{\varphi(m)}$ とおき、$1, 2, \ldots, n$ のうち、n と互いに素な数を、$b_1, b_2, \ldots, b_{\varphi(n)}$ とおく。

このとき、$(m, n) = 1$ であるので、

$$\begin{cases} c \equiv a_i \bmod m \\ c \equiv b_j \bmod n \end{cases} \tag{3}$$

を満たす c が法 mn の元で一意に定まる。この c は、mn と互いに素であることを示すことができる。なぜなら、もし、$(c, mn) > 1$ とすると、c は m か n の素因数のひとつを素因数として有していることになるが、これは、a_i が m と互いに素であること、あるいは、b_j が n と互いに素であることに矛盾するからである。例えば、c と m が共通な素因数 p を有していたとすると、$c \equiv a_i \bmod m$ から a_i もまた素因数 p を有することになる。以上のことから、(a_i, b_j) の組をひとつ決めると（決め方は、$\varphi(m)\varphi(n)$ 通りある）、それに対応する c がひとつ決まり (明らかにそれらは全て異なる)、それは mn と互いに素であることがわかった。

逆に、$(c, mn) = 1$ である任意の c を選ぶと、それは $(c, m) = 1$ かつ $(c, n) = 1$ となるので、式 (3) を解いて得られる c のどれかに一致しているはずである。

式 (1) と式 (2) の性質を利用すると、一般の n の場合にオイラーの関数の値を計算することができる。

定理 5 自然数 n が、$n = p^\alpha q^\beta r^\gamma \cdots$ と素因数分解されるとき、

$$\varphi(n) = n(1 - \frac{1}{p})(1 - \frac{1}{q})(1 - \frac{1}{r})\cdots \tag{4}$$

である。

(証明) $p^\alpha, q^\beta, r^\gamma, \cdots$ はそれぞれ互いに素であるので、式 *(2)* の関係を繰り返し用いて、

$$\varphi(n) = \varphi(p^\alpha)\varphi(q^\beta)\varphi(r^\gamma)\cdots$$

となる。次に、式 *(1)* の関係を用いると、

$$\begin{aligned} \varphi(n) &= (p^\alpha - p^{\alpha-1})(q^\beta - q^{\beta-1})(r^\gamma - r^{\gamma-1})\cdots \\ &= p^\alpha q^\beta r^\gamma \cdots (1 - \frac{1}{p})(1 - \frac{1}{q})(1 - \frac{1}{r})\cdots \\ &= n(1 - \frac{1}{p})(1 - \frac{1}{q})(1 - \frac{1}{r})\cdots \end{aligned} \tag{5}$$

となり証明できた。 □

3.　オイラーの定理

オイラーの関数を用いて表される以下の定理は重要である。

定理 6 $(a,q)=1$ であるとき、

$$a^{\varphi(q)} \equiv 1 \bmod q \tag{6}$$

*(*証明*)* $\varphi(q)$ の定義より、q を法とする既約剰余類は $\varphi(q)$ 個ある。$a_1, a_2, \ldots, a_{\varphi(q)}$ を既約代表系[1]とする。$(a,q)=1$ であるので、定理 *3* より、$aa_1, aa_2, \ldots, aa_{\varphi(q)}$ も既約代表系である[2]。従って、

$$a_1 a_2 \cdots a_{\varphi(q)} \equiv aa_1 aa_2 \cdots aa_{\varphi(q)} \bmod q$$

である。これを変形して、

$$a^{\varphi(q)}(a_1 a_2 \cdots a_{\varphi(q)}) \equiv a_1 a_2 \cdots a_{\varphi(q)} \bmod q$$

であるが、$(a_1 a_2 \cdots a_{\varphi(q)}, q) = 1$ であるから、

$$a^{\varphi(q)} \equiv 1 \bmod q$$

となり証明できた。 □

オイラーの定理の特殊な場合として、フェルマーの小定理が知られている。これは、オイラーの定理で、$q=p$（p は素数）の場合であり、a を p と互いに素な正整数として

$$a^{p-1} \equiv 1 \bmod p \tag{7}$$

が成り立つというものである。

4. オイラーの関数の性質

4.1 指数について

正整数 a に対して、$(a,q)=1$ であるとき、$a^e \equiv 1 \bmod q$ である最小の正整数 e を a の指数と呼ぶ。指数に関して、以下の定理が成り立つ。

定理 7 e を法 q の元での a の指数とする。このとき、

$$a^n \equiv 1 \bmod q$$

であれば、$e|n$ である。

（証明） $e \nmid n$ であると仮定する。すなわち、

$$n = qe + r \ (0 < r < e)$$

とおく。すると、

$$1 \equiv a^n \equiv a^{qe+r} \equiv a^{qe}a^r \equiv a^r$$

となるので、e が指数であることに矛盾する。従って、$e|n$ である。 □

この定理 7 と定理 6 とから、

$$e|\varphi(q)$$

が成立することもわかる。

4.2 オイラーの関数の和

自然数 n に対して、次の公式が成り立つ。

$$\sum_{d|n} \varphi(d) = n \tag{8}$$

上式で、和は $d|n$ である d（つまり n の約数）について取ることを意味している。

これは、n との最大公約数が d であるような数 $r(0 < r \le n)$ の集合を $\mathcal{C}_d$ と書くことにすると、明らかに $\mathcal{C}_d \cap \mathcal{C}_{d'} = \phi(d \ne d')$ かつ $\cup \mathcal{C}_d = \{1, 2, \ldots, n\}$ であることから、

$$\sum_{d|n} |\mathcal{C}_d| = n$$

となることから導かれる。（$|\mathcal{C}_d|$ は、集合に含まれる要素の数を表す。）いま、$r = id$ とおけば、$(r,n)=d$ である r の数（$|\mathcal{C}_d|$）は、

$$(i, \frac{n}{d}) = 1 \ (0 < i \le \frac{n}{d})$$

となる i の数に等しくなる。従って、この数は、$\varphi(\frac{n}{d})$ であることがわかる。一方、(r,n) は各 $r(0 < r \le n)$ について n を割りきるので、

$$\sum_{d|n} \varphi(\frac{n}{d}) = n$$

となる。この式は、式 (8) の和をとる順番を入れ替えただけであり、式 (8) と等価であることがわかる。

[1] $\varphi(q)$ 個の既約剰余類から要素を 1 つずつ選んで得られる集合のこと。

[2] 定理 3 は既約代表系について述べたものではないが、$(a,q)=1$ かつ $(b,q)=1$ であるとき $(ab,q)=1$ であることに注意すれば、既約代表系に関しても定理 3 が成り立つことがわかる。

4.3 一次合同式の解法

定理 6 より、

$$a \cdot a^{\varphi(q)-1} \equiv 1 \bmod q$$

であるので、$(a, q) = 1$ の時の一次合同式

$$ax \equiv b \bmod q$$

の解 x は

$$x \equiv a^{\varphi(q)-1} b \bmod q$$

とオイラーの関数を用いて表すことができる。