7 Euler の定理

入学年度		学部	学 科		組		番　号			検	フリガナ	
		B		1							氏 名	

m を法とする合同類全体の集合 $\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$ は和・差・積が定義された集合であり，剰余環と呼ばれのであった．さらに，m が素数 p の場合には $\mathbb{Z}/p\mathbb{Z}$ は 0 以外の除法が可能であり，有限体と呼ばれ，$\mathbb{F}_p$ と表される．しかし，m が合成数の場合には $\mathbb{Z}/m\mathbb{Z}$ は零因子をもち，必ずしも除法が可能でるとは限らない．

一般に，2 つの整数 m, n の最大公約数 $\gcd(m, n)$ が 1 に等しいとき，m と n は**互いに素**であるという．いま，

$$(\mathbb{Z}/m\mathbb{Z})^\times = \{\overline{n} \mid n \text{ と } m \text{ は互いに素 }\}$$

定義する．ユークリッドの互除法によるアルゴリズムにより，n と m が互いに素であるとき，$ax + my = 1$ を満たす整数 x，y が存在する．したがって，このとき，$nx \equiv 1 \pmod{m}$ となる整数 x が存在することがわかる．これは $\mathbb{Z}/m\mathbb{Z}$ において，$\overline{n}$ は逆元 n^{-1} を持つことに他ならない．すなわち，

$$(\mathbb{Z}/m\mathbb{Z})^\times = \{\overline{n} \mid \overline{n} \text{ は逆元を持つ }\}$$

以後，$\mathbb{F}_p$ の場合と同様，$(\mathbb{Z}/m\mathbb{Z})^\times$ の元は $\overline{\ }$ なしで書くことにする．$(\mathbb{Z}/m\mathbb{Z})^\times$ は乗法について閉じていることは容易にわかる．

例 1. $(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$．この場合 $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$ であるから，$3^{-1} = 3$, $5^{-1} = 5$, $7^{-1} = 7$ が成り立つ．

×	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

表 1　$(\mathbb{Z}/8\mathbb{Z})^\times$ の乗法表

1　$(\mathbb{Z}/4\mathbb{Z})^\times$, $(\mathbb{Z}/6\mathbb{Z})^\times$, $(\mathbb{Z}/9\mathbb{Z})^\times$, $(\mathbb{Z}/10\mathbb{Z})^\times$ を求めよ

2　a)　$(\mathbb{Z}/15\mathbb{Z})^\times$ を求め，その元の個数を求めよ．

b)　$(\mathbb{Z}/15\mathbb{Z})^\times$ の乗法表を作れ．

×	1							
1								

表 2　$(\mathbb{Z}/15\mathbb{Z})^\times$ の加法表

c)　$(\mathbb{Z}/15\mathbb{Z})^\times$ のすべての元の積を N とおく．N は逆元を持つことを示せ．

d)　$(\mathbb{Z}/15\mathbb{Z})^\times$ の元の個数を f とする．$(\mathbb{Z}/15\mathbb{Z})^\times$ の任意の元 a について，$a^f = 1$ が成り立つことを証明せよ．上の表の各行には $(\mathbb{Z}/15\mathbb{Z})^\times$ の各元が 1 度ずつ現れることを用い，Fermat の小定理と同様にすればよい．

【裏に続く】

正の整数 m に対し，m と互いに素である 1 以上 m 以下の整数の個数を $\varphi(m)$ で表す．$\varphi(m)$ は $(\mathbb{Z}/m\mathbb{Z})^\times$ の元の個数に他ならない．関数 $\varphi(m)$ は **Euler （オイラー）の関数**と呼ばれる．表の問題で示したことは，Fermat の小定理の拡張である次の定理が成り立つ．

Euler の定理

a を m と互いに素な数とするとき，

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

が成り立つ．

3 $\varphi(m)$ を $m = 2, 3 \ldots, 12$ について求めよ．

4 p は素数とする．

a) $\varphi(p)$ を求めよ．

b) $\gcd(n, p^2) \neq 1$ となる整数 n $(1 \leq n \leq p^2)$ の個数を求めよ．

c) $\varphi(p^2)$ を求めよ．

d) k を正の整数とするとき，$\gcd(n, p^k) \neq 1$ となる整数 n $(1 \leq n \leq p^k)$ の個数を求め，$\varphi(p^k)$ を求めよ．

5 $\varphi(15)$ を求め，$\varphi(15) = \varphi(3)\varphi(5)$ であることを示せ．

6 p, q を素数とするとき，pq と互いに素でない数を数えることにより，$\varphi(pq)$ を求めよ．

7 $\varphi(36)$ を求め，$\varphi(36) = \varphi(4)\varphi(9)$ であることを示せ．

8 【やや難】

a) m と n が互いに素であるとき，$\varphi(mn) = \varphi(m)\varphi(n)$ が成り立つことを示せ．

b) p を素数とするとき，$\varphi(p^k) = p^k\left(1 - \dfrac{1}{p}\right)$ であることを示せ．

c) 正の整数 m が $m = p_1^{e_1} p_2^{e_2} \cdots p_d^{e_d} = \prod_{k=1}^{d} p_k^{e_i}$ と因数分解されるとき，

$$\varphi(m) = p \prod_{k=1}^{d} \left(1 - \frac{1}{p_k}\right)$$

が成り立つことを証明せよ．

担当：鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)