3 $\mathbb{F}_p$ 上の多項式環

入学年度	学部	学科	組	番号	検	フリガナ	
		1				氏名	

• $\mathbb{F}_p$ 係数の多項式

高校数学で扱う多項式（＝整式）と同様，$\mathbb{F}_p$ の元を係数とする多項式（$\mathbb{F}_p$ 上の多項式と呼ぶ）についても，除法が可能である．すなわち，$\mathbb{F}_p$ 係数の多項式 $A(x)$，$B(x)$ について，

$$A(x) = B(x)Q(x) + R(x), \qquad \deg R(x) \leqq \deg Q(x)$$

をみたす $\mathbb{F}_p$ 係数の多項式 $Q(x)$ と $R(x)$ を一意的に求める事ができる．ただし，deg は多項式の次数を表す．また，高校数学で習った「剰余の定理」「因数定理」も同様に成り立つ．さらに，因数分解の一意性なども成り立つ．詳しいことは代数学の教科書の多項式環の章を参照のこと．

例えば，$p = 5$ として，$\mathbb{F}_5$ 係数の多項式 $F(x) = x^2+2x+2$ を考える．いま，$F(1) = 1+2+2 = 5 \equiv 0 \pmod 5$, $F(2) = 4+4+2 = 10 \equiv 0 \pmod 5$ であるから，因数定理により，$x-1, x-2$ が $F(x)$ の因数であることがわかる．$F(x)$ の次数と，x^2 の係数を考慮して

$$x^2 + 2x + 2 = (x-1)(x-2) \qquad (\mathbb{F}_5 \text{ 係数の多項式として})$$

が成り立つ．これはまた $x^2 + 2x + 2 = (x+4)(x+3)$ とも表せることに注意．

1 次の $\mathbb{F}_5$ 係数の多項式を因数分解せよ．

a) $x^2 + x + 3$　　b) $x^2 + 1$

c) $x^2 + x + 1$　　d) $x^2 + x + 4$

e) $x^3 + x^2 + x + 1$　　f) $x^4 - 1$

2 次の $\mathbb{F}_7$ 係数の多項式を因数分解せよ．

a) $x^2 + x + 1$　　b) $x^2 + 1$

c) $x^2 - x + 1$　　d) $x^6 - 1$

$x^2 - 1$ を $\mathbb{F}_p$ 上の多項式とみる．p がどんな素数であっても，明らかに $x^2 - 1 = (x-1)(x+1)$ は成り立つ．ただし，$p = 2$ の場合は $-1 \equiv 1 \pmod 2$ なので，$\mathbb{F}_2$ 上では $x^2 - 1 = (x-1)^2$ となり，他の素数の場合とは様子が異なる．そこで，以下では p は **2 以外**の素数とする．

3 a) $\mathbb{F}_p^\times$ の元 a で，$a^2 = 1$ となるものは $a = 1$ または $a = p-1$ に限ることを示せ．

b) $\mathbb{F}_p^\times$ の元 a で，$a = a^{-1}$ となるものは $a = 1$ または $a = p-1$ に限ることを示せ．

p 元体 $\mathbb{F}_p$ の可逆元全体の集合 $\mathbb{F}_p^\times$ は，a とその逆元 a^{-1} をペアにした $\{a, a^{-1}\}$ という形の集合に分割すると，

$$\{1, 1^{-1}\} = \{1\}, \quad \{2, 2^{-1}\}, \quad \{3, 3^{-1}\}, \ \ldots, \ \left\{p-1, (p-1)^{-1}\right\} = \{p-1\}$$

と $\frac{p+1}{2}$ 個の集合に分割される．たとえば，$p = 11$ とすると，

$$\{1\}, \quad \{2, 6\}, \quad \{3, 4\}, \quad \{5, 9\}, \quad \{7, 8\}, \quad \{10\}$$

と $\frac{11+1}{2} = 6$ 個に分割される．ここでのポイントは，1 と $p-1 = -1$ 以外は，a とその逆数 a^{-1} が等しくなることはないということである．

4 $p = 13$ の場合に $\mathbb{F}_{13}^\times$ を実際にこのように分割してみよ．$p = 17, 19$ の場合にはどうなるか．

【裏に続く】

5 p 元体 $\mathbb{F}_p$ の可逆元全体の集合 $\mathbb{F}_p^\times$ は，a とその逆元 a^{-1} をペアにすることにより，

$$\{1\},\quad \{2,2^{-1}\},\quad \{3,3^{-1}\},\ \ldots,\ \{p-1\}$$

と $\frac{p+1}{2}$ 個の集合に分割されることを用い，$(p-1)!$ を順序を変えて計算することにより，Wilson の定理と呼ばれる次の式を証明せよ．

$$(p-1)! \equiv -1 \pmod{p}$$

普通の整数では，任意の a について $a, a^2, a^3, \ldots, a^k, \ldots$ と計算していくと，その絶対値はどんどん大きくなり発散していく．しかし，有限個の元しか持たない p 元体 $\mathbb{F}_p$ では，$a, a^2, a^3, \ldots, a^k, \ldots$ のすべてが閉じた $\mathbb{F}_p$ に納まるので，「鳩の巣原理」あるいは「部屋割り論法」により，$k \neq l$ であって $a^k = a^l$ となることが起きないわけにはいかない．そこで，$\mathbb{F}_p$ でのべき乗 a^k の様子を見るために，まず $p = 5$ として，$\mathbb{F}_5^\times$ の各元 a について a^k $(k = 1, 2, \ldots)$ を計算してみると，次のような表が出来る．

a \ k	1	2	3	4	5	6	…
1	1	1	1	1	1	1	…
2	2	4	3	1	2	4	…
3	3	4	2	1	3	4	…
4	4	1	4	1	4	1	…

6 a) $p = 7$ として，$\mathbb{F}_7^\times$ の各元 a について上と同じような表を作れ．

a \ k	1	2	3	4	5	6	7	8	9	…
1										…
2										…
3										…
4										…
5										…
6										…

b) 左下の表の $k = 6$ の列と $k = 3$ の列に注目してその特徴を述べよ．

c) 上で見た特徴を際立たせるために，$6 \equiv -1 \pmod 7$ であることなどより，$\mathbb{F}_7^\times = \{\pm1, \pm2, \pm3\}$ として，上の表を書き直してみよ．

a \ k	1	2	3	4	5	6
1						
2						
3						
−3						
−2						
−1						

7 $p = 11$ とし，$\mathbb{F}_{11}^\times = \{\pm1, \pm2, \pm3, \pm4, \pm5\}$ と表して，a^k の表を作れ．

a \ k	1	2	3	4	5	6	7	8	9	10
1										
2										
3										
4										
5										

一般に次の性質が成り立つ．

Fermat の小定理

p を素数とし，a を p と互いに素な整数とする．このとき，次の合同式が成り立つ．

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

ここで，p が素数であることが重要で，素数でない整数 m を法とし場合は同様の性質は成り立たない．

8 $2^{9-1} \pmod 9$，$2^{12-1} \pmod{12}$，$2^{15-1} \pmod{15}$ を計算せよ．

担当：鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)