教育課題演習　第 8 回　有限体 F_p

1．剰余の表を作る

整数 a を正の整数 k で割った余りを $a \bmod k$ で表す。

a \ b	0	1
0	0	0
1	1	0

$(a+b) \bmod 2$

a \ b	0	1
0	0	0
1	0	1

$(a\times b) \bmod 2$

a \ b	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$(a+b) \bmod 3$

a \ b	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$(a\times b) \bmod 3$

a \ b	0	1	2	3	4
0					
1					
2					
3					
4					

$(a+b) \bmod 5$

a \ b	0	1	2	3	4
0					
1					
2					
3					
4					

$(a\times b) \bmod 5$

a \ b	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

$(a+b) \bmod 7$

a \ b	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

$(a\times b) \bmod 7$

２．整数の合同

2 数 a, b を正の数 k で割った余りが等しいとき，a, b は k を法として合同であるといい，　$a \equiv b \bmod k$ で表す。

a を正の数 k で割った余り r は，以下の等式，不等式を満たす。

$$a=kq+r \ (q \text{ は整数}), \quad 0 \leqq r < k$$

例

$9 \equiv 4 \equiv -1 \equiv -6 \bmod 5$

合同式の基本性質

$a \equiv b \bmod k$，$c \equiv d \bmod k$ ならば，$a+c \equiv b+d \bmod k$，$ac \equiv bd \bmod k$

証明

$$a \equiv b \bmod k \ \Leftrightarrow \ a-b \text{ は } k \text{ の倍数}$$

を示し，この関係を利用する。

３．剰余系

k を 1 より大きい整数とする。

集合$\{ 0, 1, 2, \cdots, k-1 \}$に，加法$\oplus$を $a \oplus b=(a+b) \bmod k$，乗法$\otimes$を $a \otimes b=ab \bmod k$ によって定めてできる代数系を，k を法とする剰余系という。

剰余系の基本性質

(1)　$(a \oplus b) \oplus c=a \oplus (b \oplus c)$,　$(a \otimes b) \otimes c=a \otimes (b \otimes c)$　　(結合法則)

(2)　$a \oplus b=b \oplus a$,　　$a \otimes b=b \otimes a$　　(交換法則)

(3)　$a \otimes (b \oplus c)=(a \otimes b) \oplus (a \otimes c)$　　(分配法則)

(4)　$a \oplus 0=a$,　　$a \otimes 1=a$　　(加法，乗法の単位元の存在)

(5)　$a \oplus x=0$ となる x が存在する。　　（加法に関する逆元の存在）

$a \oplus x=0$ となる x は，具体的には，$x=(-a) \bmod k$ 。

さらに法が素数であれば,

(6)　$a \neq 0$ のとき，$a \otimes x=1$ となる x が存在する。　（乗法に関する逆元の存在）

問題１

7 を法とする剰余系において，1,2,3,4,5,6 の各数の乗法に関する逆元を求めよ。

問題２（スキップ可）

k が素数であるとき，k を法とする剰余系において，0 以外の各要素は乗法に関する逆元を持つことを示せ。

ヒント　a, b が互いに素な自然数であるとき，$ax+by=1$ となる整数 x,y が存在する。

(1)～(6)が成立する代数系を**体**という。有理数全体や実数全体も体の例である。特に，要素の個数が有限の体を**有限体**という。素数を法とする剰余系は有限体の例である。

４．原始根

以後，$a+b$ は $(a+b) \bmod k$ を，$a \times b$ は，$ab \bmod k$ を表すものとする。

また，累乗も剰余系における乗算の累積の意味で用いる。

たとえば，5 を法とする剰余系において，

$2^1=2$,

$2^2=4$,

$2^3=4\times2=8=3$,

$2^4=3\times2=6=1$。

$3^1=3$,

$3^2=4$,

$3^3=4\times3=12=2$,

$3^4=2\times3=6=1$。

$4^1=4$,

$4^2=1$。

0 以外のすべての要素を α^n（n は自然数）の形に表せるとき，α を原始根という。

例　5 を法とする剰余系において，2 と 3 は原始根であり，4 は原始根でない。

問題３　2, 3, 7, 11, 13 を法とする各剰余系における原始根をすべて求めよ。

５．フェルマーの小定理

5 を法とする剰余系において，$2^4=1$，$3^4=1$，$4^4=(4^2)^2=1$ となっている。

一般に，素数 p を法とする剰余系において，　$a^{p-1}=1$ $(a=1, 2, \cdots, p-1)$　となることが知られている（フェルマーの小定理)。