１０．環と体２

代数１

行列算

- 可換律は不成立

$$AB \neq BA$$

- 零因子が存在

$$AB = O \quad (A \neq O, B \neq O)$$

- 簡約律は不成立

$$AC = BC, C \neq O$$

$A = B$とは限らない

剰余類

- 整数全体をmで割った余りで生成される集合

$$Z_m = \{0,1,2,\cdots,m-1\} \pmod{m}$$

法p（素数）の剰余類

$$Z_p = \{0,1,2,\cdots,p-1\} \pmod{p}$$

- 体となる　剰余体
- 例p=5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

フェルマーの定理

$a \equiv 0 \pmod{p}$以外に対して

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

$$3^{7-1} = 3^6 = 729 = 104 * 4 + 1 \equiv 1 \pmod{7}$$

既約剰余群

$$Z_p^* = Z_p - \{0\} = \{1,2,\cdots,p-1\} \pmod{p}$$

- 例　p=7のとき