13. 剰余環

代数Ⅱ

剰余環

剰余類・・・整数をmで割った余りの集合

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

環

2つの演算（加法と乗算とすれば）に対して

(1)加法に関して群

(2)乗法に関して結合律

(3)乗法単位元が存在

(4)分配律

体

環に対して除算が成立

すなわち

(1)零元以外が可逆元

→（斜体）

(2)乗法に関して可換

法4の剰余類（剰余環）

$$Z_4 = \{0,1,2,3\}$$

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

加法群
加法単位元　0

加法において逆元が存在
0については0
1については3
2については2
3については1

乗法に関して結合律を満たす

乗法単位元　1

加法と乗法に関して分配律を満たす

$$x(y+z) = xy + xz$$

例)　$1(2+3) = 2+3 = 1$

x	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

零因子
2・2=0から2
整域ではない

既約剰余類

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

法mの剰余類の中で，mと互いに疎となる元のみの集合

$$Z_m^*$$

素数pを法とする剰余類の場合は0を除いた集合と同じとなる

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

フェルマーの定理

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

$Z_6^* = \{1,5\}$

2，3，4に対しては，何乗しても1にはならない

例題

- （P.161）463□は6の倍数である
  6の倍数＝2の倍数かつ3の倍数
  3の倍数は九去法と同様に考えられる.
  $4+6+3+x=13+x\equiv 1+x(\mathrm{mod}\ 3)$
  2,5,8 のいずれかであるが，2の倍数なので，
  で，2か8が答えとなる.

合同式の利用

- 1次不定方程式
  $$ax+by=c$$
- 解が存在　⇔　$(a,b)|c$　　cは(a,b)の倍数
- 1次不定方程式の両辺を法bで合同式を取る
  $$ax=c(\mathrm{mod}\ b)$$

この合同式を解くことで，答えが出る.

例　$3x+5y=1$

$3x=1(mod\ 5)$より，3の逆数2を掛けて，

$x=5k+2$とあらわされる．$y=-3k-1$

問題

- 次の問題に答えはあるか，あれば求めよ．

(1) $9x + 15y = 6$
(2) $8x + 12y = 5$
(3) $31x + 56y = 3$
(4) $3x^2 - x \equiv 2 (\mathrm{mod}\ 7)$
(5) $41x + 310y = 10$