4. 剰余環
有理整数環，合同式の利用

代数 II

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

有理整数環

- 整数の世界
  - 加法と乗法に関する基本的性質

(1)a,b,cをZの元とすれば,$(a+b)+c=a+(b+c)$

(2)a,bをZの元とすれば，$a+b=b+a$

(3)Zの任意の元aに対して,$0+a=a+0=a$

(4)Zの任意の元aに対して，$x+a=a+x=0$を満たすZの元xが存在

(5)a,b,cをZの元とすれば,$(ab)c=a(bc)$

(6)a,bをZの元とすれば，$ab=ba$

(7)Zの任意の元aに対して$1a=a1=a$

(8)a,b,cをZの元とすれば,$(a+b)c=ac+bc$

(9)a,bをZの元とするとき，$ab=0$ならば$a=0$または$b=0$

(10)a,bをZの元とするとき,

$a>b,a=b,a<b$

のどれか1つだけが成立

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) $41x + 310y = 10$