● 剰余環

整数全体の集合を $\mathbb{Z}$ で表す．m を正の整数とするとき，「m を法として合同」という関係を考えると，整数全体の集合 $\mathbb{Z}$ を m 個のグループ（部分集合）に分けることができる．すなわち，2 つの整 a と b に対して $a \equiv b \pmod m$ が成り立つとき a と b は同じグループに属すると定める．例えば，2 を法として合同という関係を用いると，すべての整数を偶数と奇数という 2 つのグループに分けることができる．すなわち，

$$\mathbb{Z} = \{\cdots, -2, 0, 2, 4, 6, \cdots\} \cup \{\cdots, -3, -1, 1, 3, 5, \cdots\}$$

すべての整数を下 1 桁の数で分類することは 10 を法として合同という関係による分類に他ならない．また，日にちを整数で表しておけば，7 を法とする合同という関係で曜日という 7 つのグループに分けることができる．いま，正の整数 m を固定し，m を法として合同という関係でグループに分けるとき，整数 a の属するグループのことを $\overline{a}$ と書き表す．任意の整数は

$$\overline{0},\ \overline{1}, \overline{2}, \ldots, \overline{m-1},$$

という m 個のグループのどれかに属すので，整数全体は m 個のグループに分けられる．$\overline{a}$ は m **を法とする** a **の合同類** と呼ばれる．以前扱った合同式の性質を用いると，合同類の間で和や積を考えることが出来る．すなわち，

$$\overline{a} + \overline{b} = \overline{a+b}, \quad \overline{a}\,\overline{b} = \overline{ab}$$

と定義することができる．例えば，$m = 2$ とすると，整数全体は $\overline{0}$ = (偶数全体) と $\overline{1}$ = (奇数全体) の 2 つの合同類の間の，和と積の演算は以下の表にまとめられる．

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\times$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

$\overline{1} + \overline{0} = \overline{1}$ や $\overline{1} \times \overline{0} = \overline{0}$ という式は，(奇数) + (偶数) = (奇数) や (奇数) × (偶数) = (偶数) という性質をシンプルな記号で書き表すことにほかならない．2 を法とする合同類を考えていることが明らかな場合は $^-$ をとってさらに簡単に表すことも多く，慣れれば便利である．

1　a) 6 を法とする合同類の間の足し算とかけ算の表を作れ．

$+$	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

$\times$	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

入学年度		学部	学科		組		番号			検	フリガナ	
		D		1							氏名	

b) 7 を法とする合同類の間の足し算とかけ算の表を作れ．

$+$	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

$\times$	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

c) $a = 1, \ldots, 6$ のすべてについて，$ax \equiv 1 \pmod 7$ となる x を表から読み取れ．

d) $ax \equiv 1 \pmod 6$ となる x が存在するためには，a がどのような条件を満たさなければならないか．

m を法とする合同類全体の集合を $\mathbb{Z}/m\mathbb{Z}$ という記号を使って表す．

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$$

m を法とする合同類を扱っていることが明らかである場合には $\mathbb{Z}/m\mathbb{Z} = \{0, 1, \ldots, m-1\}$ と $^-$ なしで書くことも多い．$\mathbb{Z}/m\mathbb{Z}$ は和・差・積が定義された集合である．一般に和・差・積が定義され結合法則，分配法則が満たされている集合を「**環**」と呼ぶ．$\mathbb{Z}/m\mathbb{Z}$ は環であり，**剰余環**と呼ばれる．

環の元 a, b が次の条件

$$a \neq 0, \quad b \neq 0 \quad \text{かつ} \quad ab = 0$$

を満たすとき，a，b を**零因子**と呼ぶ．例えば，$\mathbb{Z}/6\mathbb{Z}$ において $\overline{3}$ は零因子である．

2　a) $\mathbb{Z}/6\mathbb{Z}$ の零因子を求めよ．

b) $\mathbb{Z}/8\mathbb{Z}$ のすべての零因子を求めよ．

c) $a \in \mathbb{Z}/8\mathbb{Z}$ が零因子でないとき，$ax \equiv 1 \pmod 8$ を満たす x を求めよ．

【裏に続く】

3 剰余環 $\mathbb{Z}/m\mathbb{Z}$ $(m>1)$ において，「$\mathbb{Z}/m\mathbb{Z}$ が零因子をもたない」ための必要十分条件は「m は素数」であることを証明せよ

- p 元体

以後，特に断りのない限り，p と書けばそれは素数を表すこととする．p を法とする合同類からなる剰余環 $\mathbb{Z}/p\mathbb{Z}=\{\overline{0},\overline{1},\ldots,\overline{p-1}\}$ については，前回の練習問題の内容を言い換えると，次の性質が成り立つ．

(1) $\mathbb{Z}/p\mathbb{Z}$ は零因子を持たない．
(2) $\overline{a}\neq\overline{0}$ ならば，$\overline{a}\,\overline{x}=\overline{1}$ をみたす $\overline{x}$ が存在する．
(3) $\overline{a}\neq\overline{0}$ ならば，任意の $\overline{b}$ に対して $\overline{a}\,\overline{x}=\overline{b}$ をみたす $\overline{x}$ が存在する．

例えば，$p=7$ とすると，$2\times4\equiv1\pmod 7$ であるから，$\overline{2}\times\overline{4}=\overline{1}$ と書くことができる．これは，$\overline{4}$ が $\overline{2}$ の「逆数」の役割を担っていることを意味する．一般に，$\overline{a}\,\overline{x}=\overline{1}$ をみたす $\overline{x}$ を $\overline{a}$ の**逆元**といい，$\overline{a}^{-1}$ と表す．たとえば，$\overline{4}=\overline{2}^{-1}$ である．もちろん $\overline{2}=\overline{4}^{-1}$ でもある．誤解の恐れがない場合は，$\overline{\ }$ をとって，「$\mathbb{Z}/7\mathbb{Z}$ において $2^{-1}=4$ である」と表す．

4 $\mathbb{Z}/7\mathbb{Z}$ の 0 以外の各々の元について、その逆元を求めよ．

$1^{-1}=$　　$2^{-1}=$　　$3^{-1}=$　　$4^{-1}=$　　$5^{-1}=$　　$6^{-1}=$

普通，1 次方程式 $ax=b$ を解くには，両辺を a で割って，$x=\frac{b}{a}$ とするが，これは両辺に逆数 a^{-1} をかけ $x=ba^{-1}$ とすることと言い換えられる．$\mathbb{Z}/7\mathbb{Z}$ 内の方程式 $ax=b$ についても同様に，方程式の両辺に a の逆元 a^{-1} をかけて解くことができる．すなわち，$x=ba^{-1}$ が解である．例えば，$3x=4$ であれば，この両辺に $3^{-1}=5$ をかけて，$x=4\times3^{-1}=4\times5=20=6$ となる．実際，$x=6$ のとき，$3x\equiv3\times6\equiv18\equiv4\pmod 7$ であり，確かに解である．

5 $p=11$ として，$\mathbb{Z}/11\mathbb{Z}$ について考える．

a) $\mathbb{Z}/11\mathbb{Z}$ の 0 以外の各々の元に付いて，その逆元を求めよ．

$1^{-1}=$　　$2^{-1}=$　　$3^{-1}=$　　$4^{-1}=$　　$5^{-1}=$

$6^{-1}=$　　$7^{-1}=$　　$8^{-1}=$　　$9^{-1}=$　　$10^{-1}=$

b) $\mathbb{Z}/11\mathbb{Z}$ における次の方程式を解け．

a) $3x=4$　　b) $5x=10$　　c) $7x=6$

担当：鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)

一般に，p を法とする剰余環 $\mathbb{Z}/p\mathbb{Z}$ は $\mathbf{F}_p$ はとも表され，p **元体**と呼ばれる．混同の恐れがないときは，$\overline{\ }$ をとって簡単に表すので，

$$\mathbf{F}_p=\mathbb{Z}/p\mathbb{Z}=\{0,1,2,\ldots,p-1\}$$

である．$\mathbf{F}_p$ は加法・減法について閉じている．さらに，$\mathbf{F}_p$ から $\overline{0}=0$ を除いた集合

$$\mathbf{F}_p^{\times}=\{1,2,\ldots,p-1\}$$

は乗法についても閉じており，上の性質 (2) により各元が逆元を持つことから，除法についても閉じていることが示される．

日頃我々が「数」と呼ぶものを特徴づける最も重要な性質は四則演算ができることである．とくに，有理数や実数は 0 以外の数による除法が必ずできる．現代数学では，このように除法まで含めた四則演算について閉じている集合はすべて「数の体系」であると考える．このような四則演算が定義された集合は「**体**」（独：Korper，仏：corps，英：field）と呼ばれる．$\mathbf{F}_p$ も新たな数の体系と見做され，p 個の元（要素）をもつ体であることから p 元体と呼ばれる．

もう少し抽象的・形式的に正確に定義すると，体とは以下のように定義される．

「体」の定義

集合 K の任意の二つの元 a,b に対し，その**和** $a+b$ と**積** ab と呼ばれる K の元がそれぞれ定義され，次の（K 1）から（K 10）までの条件をみたすとき，K は**体**であるという．

(K 1)【和の交換律】任意の a,b について，$a+b=b+a$.
(K 2)【和の結合律】任意の a,b,c について $(a+b)+c=a+(b+c)$.
(K 3)【加法の単位元 0 の存在】0 で表される K の元が存在し，すべての K の元 a に対して $a+0=a$ をみたす．
(K 4)【加法の逆元の存在】任意の K の元 a に対して $-a$ で表される K の元が存在し，$a+(-a)=0$ をみたす．
(K 5)【積の交換律】任意の a,b について，$ab=ba$.
(K 6)【積の結合律】任意の a,b,c について，$(ab)c=a(bc)$.
(K 7)【分配律】 任意の a,b,c について，$a(b+c)=ab+ac$.
(K 8)【乗法の単位元 1 の存在】1 で表される K の元が存在し，すべての $\mathbf{R}$ の元 a に対して $a1=a$ をみたす．
(K 9)【乗法の逆元の存在】0 でない任意の $\mathbf{R}$ の元 a に対して a^{-1} または $1/a$ で表される $\mathbf{R}$ の元が存在し，$aa^{-1}=1$ をみたす．
(K 10)【0 以外の元の存在】 $1\neq0$.

有理数全体の集合 $\mathbb{Q}$，実数全体の集合 $\mathbb{R}$，複素数全体の集合 $\mathbb{C}$ はすべて体である．一方，整数全体の集合 $\mathbb{Z}$ は体ではない．剰余環 $\mathbb{Z}/m\mathbb{Z}$ は m が素数であるときに限り (K 4) をみたし，$\mathbf{F}_p=\mathbb{Z}/p\mathbb{Z}$ は体である．

(K 3), (K 8), (K 10) により，体 K は必ず 0 と 1 という異なる元をもつから，空集合 ϕ や $\{0\}$ は体ではない．したがって，$\mathbf{F}_2=\{0,1\}$ が最も小さい体ということになる