入学年度	学部	学科	組	番号	検	フリガナ	
		1				氏名	

● 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 個の類（部分集合）に分けることができる．すなわち，2つの整数 a と b に対して $a \equiv b \pmod m$ が成り立つとき a と b は同じ類に属すると定める．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 つの類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 つの類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類に分けるとき，整数 a の属する類のことを **m を法とする a の合同類** と呼び，$\overline{a}$ または $a \bmod m$ などと表す．整数全体は

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

という m 個の類に分けられる．合同式の基本的な性質を用いると，合同類の間の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．法とする整数 m が明らかな場合は $\overline{a}$ の代わりに $\bar{}$ をとって単に a と表すことも多く，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						

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すべきか．

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 $\bar{}$ 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) $\mathbb{Z}/6\mathbb{Z}$ の零因子をすべて求めよ．

b) $\mathbb{Z}/8\mathbb{Z}$ の零因子をすべて求めよ．

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】

ユークリッドの互除法によるアルゴリズムにより，任意の整数 a と m について，その最大公約数を d としたとき，$ax + my = d$ を満たす整数 x，y を求めることができる．とくに，a と m が互いに素であるとき，すなわち a と m の最大公約数 $\gcd(a, m)$ が 1 であるとき，

$$ax + my = 1$$

を満たす整数 x，y が存在する．したがって，このとき，$ax \equiv 1 \pmod{m}$ となる整数 x が存在することがわかる．これは $\mathbb{Z}/m\mathbb{Z}$ において，

$$\overline{a}x \equiv \overline{1}$$

を満たす元 x が存在すると言い換えることができる．このような $\mathbb{Z}/m\mathbb{Z}$ の元 x を $\overline{a}$ の**逆元**という．$\overline{a}$ の逆元は $\overline{a}^{-1}$ と表されることもある．

3 m を 1 より大きい整数とするとき，「剰余環 $\mathbb{Z}/m\mathbb{Z}$ 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．上の問題より，$\mathbb{Z}/p\mathbb{Z}$ は零因子を持たない．

4 $\mathbb{Z}/p\mathbb{Z}$ について，次のことを証明せよ．

a) $\overline{a} \neq \overline{0}$ ならば，$\overline{a}\,\overline{x} = \overline{1}$ をみたす $\overline{x}$ が存在する．

b) $\overline{a} \neq \overline{0}$ 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．

担当：鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)

例として，$p = 7$ とすると，$2 \times 4 \equiv 8 \equiv 1 \pmod{7}$ 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 $\overline{2}$ の逆元であることを意味する．すなわち，$\overline{4} = \overline{2}^{-1}$ 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．

5 $\mathbb{Z}/7\mathbb{Z}$ の 0 以外の各々の元について、その逆元を求めよ．

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

ふつう，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．$\mathbb{Z}/7\mathbb{Z}$ 係数の方程式 $ax = b$ 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，$x = 4 \times 3^{-1} = 4 \times 5 = 20 = 6$ となる．実際，$x = 6$ のとき，$3x \equiv 3 \times 6 \equiv 18 \equiv 4 \pmod{7}$ であり，確かに解である．

6 $p = 11$ 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) $7x = 6$

一般に，p を法とする剰余環 $\mathbb{Z}/p\mathbb{Z}$ は体の公理をみたし，p **元体**と呼ばれ，$\mathbb{F}_p$ とか，$GF(p)$ などと表せる．混同の恐れがないときは，$\overline{\ }$ をとって簡単に表すので，

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

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

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

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．従って，$\mathbb{F}_p^{\times}$ は乗法に関して群をなす．$\mathbb{F}_p^{\times}$ は $\mathbb{F}_p$ の**乗法群**と呼ばれる．