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 $0 =$ (偶数全体) と $1 =$ (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 $\overline{\ }$ 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．このとき，上の表で普通の足し算・かけ算と異なる唯一の場合が $1 + 1 = 0$ という関係であることに注意する．

次に 5 を法とする合同類の間の足し算とかけ算の表を作ってみる．ここでは，$\overline{\ }$ なしで書いてある．

$+$	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

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

かけ算の表において，0 の行以外では，1 が必ず 1 回だけ現れることに注意する．

2024 年 4 月 25 日

入学年度		学部	学 科		組		番　号			検	フリガナ	
		B		1							氏 名	

1 $a = 1, \ldots, 4$ のすべてについて，$ax \equiv 1 \pmod{5}$ となる x を表から読み取れ．

2 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) 上の 2 つの表を眺め，共通点と相違点について考えてみよ．

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．

【裏に続く】

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 を法とする剰余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 $\overline{\ }$ 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．

3 a) $\mathbb{Z}/6\mathbb{Z}$ のその他の零因子を求めよ．

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

4 剰余環 $\mathbb{Z}/m\mathbb{Z}$ $(m > 1)$ において，m は合成数ならば $\mathbb{Z}/m\mathbb{Z}$ は零因子をもつことを証明せよ．

5 a) 8 と互いに素な a それぞれについて，$ax \equiv 1 \pmod 8$ となる x を求めよ．

b) 8 と互いに素な a と，任意の b について，$ax \equiv b \pmod 8$ となる x を求めよ．

6 p を素数とする．このとき，整数 a について，$a \not\equiv 0 \pmod p$ ならば，任意の整数 b に対して，

$$ax \equiv b \pmod p$$

を満たす $x \pmod p$ がただ 1 つ存在することを証明せよ．

前回の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のであった．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．

逆に，a と m が互いに素でなければ，その最大公約数を d とすると，$ax + my$ は d で割り切れるが，1 は d では割り切れないので，$ax + my = 1$ は解を持ち得ない．すなわち，$ax \equiv 1 \pmod m$ となる整数 x は存在せず，$\overline{a}$ は逆元を持たない．

担当：鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)