

入学年度	学部	学科	組	番号	検	フリガナ
	B	1				氏名

整数全体の集合を \mathbb{Z} で表す. m を正の整数とすると, 「 m を法として合同」という関係を考えて, 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,

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

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, 整数 a の属するグループのことを \bar{a} と書き表す. 任意の整数は

$$\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1},$$

という m 個のグループのどれかに属するので, 整数全体は m 個のグループに分けられる. \bar{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,

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

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 $\bar{0}$ (偶数全体) と $\bar{1}$ (奇数全体) の2つの合同類の間で, 和と積の演算は以下の表にまとめられる.

+	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

×	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

$\bar{1} + \bar{0} = \bar{1}$ や $\bar{1} \times \bar{0} = \bar{0}$ 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はかならない. 2を法とする合同類を考えていることが明らか場合は¹ 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での足し算とかけ算の表を作ってみる. ここでは, ¹ 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

×	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.

1) $a = 1, \dots, 4$ 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で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						

×	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

b) 7を法とする合同類の間で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							

×	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.

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.

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

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 $\mathbb{Z}/m\mathbb{Z} = \{0, 1, \dots, m-1\}$ と $\bar{\quad}$ 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 $\bar{3}$ 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, 次が成り立つことを証明せよ.

a) $\mathbb{Z}/m\mathbb{Z}$ が零因子をもつ $\Leftrightarrow m$ は合成数.

b) $\mathbb{Z}/m\mathbb{Z}$ が零因子をもたない $\Leftrightarrow m$ は素数.

5 a) a と m が互いに素であるとき, $ax + my = 1$ を満たす整数 x, y が存在することを証明せよ.

b) a と m が互いに素であるとき, $ax \equiv 1 \pmod{m}$ となる $\mathbb{Z}/m\mathbb{Z}$ の元 x が存在することを証明せよ.

6 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.

7 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.