3 p 元体

以後とくに断りのない限り，p と書けば，それは素数を表すこととする．「p を法として合同」という関係を考えると，整数全体をグループ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 $a \equiv b \pmod{p}$ 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て，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．また，7 を法として合同という関係で，すべての日は 7 つの曜日のグループに分けられる．

いま，素数 p を固定し，p 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

$$\overline{0},\ \overline{1},\ \ldots,\ \overline{p-1},\ \overline{p}$$

という p このグループのどれかに属すので，整数全体は p 個のグループに分けられる．$\overline{a}$ は p 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．

いま，$p=2$ とすると，整数全体は $\overline{0}=$ (偶数全体) と $\overline{1}=$ (奇数全体) の 2 つの合同類に分かれる．そして，和と席の演算は

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

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

$\overline{1}+\overline{0}=\overline{1}$ 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している．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．このとき，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，¯ 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．これより，$a=1,\ldots,4$ のすべてについて，$ax\equiv 1 \pmod 5$ となる x が存在することがわかる．

入学年度		学部	学 科		組		番　号			検	フリガナ	
2	3	B		1							氏 名	

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)　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．

2　Excel を用いて，17 を法とする合同類の間のかけ算の表を作れ．（「下方へコピー」，「右方へコピー」などを上手く使い，手際よく作ること．）

a)　この表を用いて $4x\equiv 1 \pmod{17}$ となる x を求めよ．また，$4x+17y=1$ となる整数の組 (x,y) を求めよ．

b)　この表を用いて $2, 2^2, 2^3, \ldots$ を計算し，最初に $2^k\equiv 1 \pmod{17}$ となる正の整数 k を求めよ．

【裏に続く】

3 同様に 23 や 101 を法とする合同類のかけ算の表を作り，p を法とする合同類のかけ算の表には次のような共通の特徴があることを観察せよ．

- 各行には 0 から $p-1$ までの数が各 1 回ずつ現れる．
- しかし，各行の数の並び方には明らかな規則はなさそうに見える．特に，1 が現れる場所はランダムなように見える．

【次週以降の話題に向けて】

4 係数が p を法とする合同類である多項式についても因数定理が成り立つ．例えば，$p=5$ として，$P(x)=x^2+2x+2$ とすると，$P(1)=1+2+2=5\equiv 0 \pmod 5$, $P(2)=4+4+2=10\equiv 0 \pmod 5$ であるから，

$$x^2+2x+2\equiv (x-1)(x-2) \pmod 5$$

が成り立つ．誤解の恐れがないときは，これを単に $x^2+2x+2=(x-1)(x-2)$ とも表す．
次の各多項式を因数分解せよ．

a) x^2+x+3　　b) x^3+x^2+x+1

5 p を法とする合同類から 0 の類を除いて作ったのかけ算の表の各行には 1 から $p-1$ までの数が各 1 回ずつ現れる．これより

$$1\times 2\times 3\times\cdots\times(p-1)\equiv -1 \pmod p$$

であることを示せ．

担当：鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)