10. 剰余類（合同式）

代数Ⅰ

合同式

$$a \equiv b \pmod{m}$$

$\Leftrightarrow a-b$がmの倍数である$\Leftrightarrow m \mid a-b$

$\Leftrightarrow a$をmで割った余り$=b$をmで割った余り

$\Leftrightarrow a$とbは法mで合同である

合同式の法則

nを1より大きい整数とする．このとき，任意の整数a,b,c,dについて，次のことが成り立つ

(1)反射律　$a \equiv a \pmod{m}$

(2)対称律　$a \equiv b \pmod{m}$ならば，$b \equiv a \pmod{m}$

(3)推移律　$a \equiv b \pmod{m}$かつ　$b \equiv c \pmod{m}$ならば　$a \equiv c \pmod{m}$

(4)　$a \equiv b \pmod{m}$かつ　$c \equiv d \pmod{m}$ならば

$a \pm c \equiv b \pm d \pmod{m}$,　$a \cdot c \equiv b \cdot d \pmod{m}$

定理

nを1より大きい整数とする．このとき，

任意の整数m, a, bに

ついて$d = (m, n), n = n'd, m = m'd$とおくとき，

次のことが成り立つ．

$$ma \equiv mb (\mathrm{mod}\, n) \Leftrightarrow a \equiv b (\mathrm{mod}\, n')$$

特に，$(m, n) = 1$のとき，

$$ma \equiv mb (\mathrm{mod}\, n) \Leftrightarrow a \equiv b (\mathrm{mod}\, n)$$

定理

a, bを整数，m, nを1より大きい整数とする．

$(m, n) = 1$であれば，次式が成り立つ．

$$a \equiv b (\mathrm{mod}\, m), a \equiv b (\mathrm{mod}\, n) \Leftrightarrow a \equiv b (\mathrm{mod}\, mn)$$

合同式の解の存在定理

$(a,n)=1$ならば，$ax \equiv b \pmod{n}$を満足する整数解xが存在し，nを法として唯1つである

$ax \equiv b \pmod{n}$が解を持つための必要十分条件は$(a,n) \mid b$となることである．

合同方程式$ax \equiv b \pmod{n}$が解を持ち$(a,n)=d>1$であるならば，解の個数はnを法としてd個である

例題

次の合同式を解こう

(1) $3x \equiv 1 \pmod{5}$

ヒント：xの係数3が1になったら，xの式になる

(2) $8x \equiv 5 \pmod{12}$

(3) $3x^2 - x \equiv 2 \pmod{7}$

ヒント：因数分解をして考える

中国剰余定理（ユークリッドの互除法）

2つの正整数$a, b(a < b)$において，大きい数bから小さい数aを引いて

$$(a, b) = (a, b - a)$$

2つの正整数$a, b(a < b)$において，大きい数bを数aで整除して

$$b = qa + r$$

$$(a, b) = (a, r)$$

$(527,901) = 17$

$$\begin{array}{r} 4 \quad 2 \quad 2 \quad 1 \quad 1 \\ 17\overline{)68)153)374)527)901} \\ \underline{68} \;\; \underline{136} \;\; \underline{306} \;\; \underline{374} \;\; \underline{527} \\ 0 \quad 17 \quad 68 \quad 153 \quad 374 \end{array}$$

剰余類の定義と定理

aを任意の整数とするとき，

$C_a = \{x \in Z \,|\, x \equiv a \pmod{n}\} = a + nZ = \{a + nt \,|\, t \in Z\}$を

nを法とするaの剰余類という．

また，nを法とする剰余類の集合をZ_nで表す．

すなわち，$Z_n = \{C_a \,|\, a \in Z\}$

nを1より大きい整数，a, bを任意の整数とするとき，

$$a \equiv b \pmod{n} \Leftrightarrow C_a = C_b$$

剰余類の性質

C_aをnを法とするaの剰余類を表すものとする.

このとき，次のことが成り立つ.

(1)$a = C_a$

(2)$C_a \cap C_b \neq \phi \Leftrightarrow C_a = C_b$

(3)Z_nは相異なるn個の元$C_0, C_1, \cdots, C_{n-1}$から構成される.

$Z_n = \{C_0, C_1, \cdots, C_{n-1}\}, C_i \cap C_j = \phi (i \neq j)$

また，このとき$Z = C_0 \cup C_1 \cup \cdots \cup C_{n-1}$となっている