１２．既約剰余類

代数１

剰余類

・整数全体をmで割った余りで生成される集合

$$Z_m = \{0,1,2,\cdots,m-1\}(\mathrm{mod}\, m)$$

法p(素数)の剰余類

$$Z_p = \{0,1,2,\cdots, p-1\} (\mathrm{mod}\ p)$$

- **法5** $Z_5 = \{0,1,2,3,4,5\} (\mathrm{mod}\, 5)$ $Z_5^{*} = \{1,2,3,4,5\} (\mathrm{mod}\, 5)$

+	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

×	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

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．

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

フェルマーの定理

素数pに対して

$$Z_p = \{0,1,2,\cdots, p-1\} (\mathrm{mod}\ p)$$

$a \equiv 0 (\mathrm{mod}\ p)$以外に対して

$$a^{p-1} \equiv 1 (\mathrm{mod}\ p)$$

$$3^{7-1} = 3^6 = 729 = 104 * 4 + 1 \equiv 1 (\mathrm{mod}\ 7)$$

既約剰余類

・素数ではないときに、既約な要素だけを抽出した集合について考える

$$Z_m = \{1,2,\cdots,m-1\} \pmod m$$

$$Z_m^{\times} = \{\text{既約な項}\} \pmod m$$

・例　m=6のとき $Z_6^{\times} = \{\overline{1},\overline{5}\}$

・例　m=8のとき $Z_8^{\times} = \{\overline{1},\overline{3},\overline{5},\overline{7}\}$

例題

例題1　10進法で表された数の各位の数字の和が3で割り切れれば，元の数が3で割り切れることを示せ．

例題2　10進法で表された数の奇数位の和と偶数位の数の和との差が11で割り切れるとき，元の整数は１１で割り切れることを示せ．

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