13. 例題

代数Ⅰ

合同式に関する定理

定理m1

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：$a \equiv a \pmod{n}$

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

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

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

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

定理m2

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

$ma \equiv mb \pmod{n} \Leftrightarrow a \equiv b \pmod{n'}$

とくに，$(m,n) = 1$のとき，$ma \equiv mb \pmod{n} \Leftrightarrow a \equiv b \pmod{n}$

定理m3

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，次のことが成り立つ

$a \equiv b \pmod{m}, a \equiv b \pmod{n} \Leftrightarrow a \equiv b \pmod{mn}$

合同式に関する定理

定理m4

$(a,n)=1$ならば，$ax\equiv b(\mathrm{mod}\,n)$を満足する整数解$x$が存在し，
nを法としてただ一つである．

定理m5

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

定理m6

合同方程式$ax\equiv b(\mathrm{mod}\,n)$が解をもち$(a,n)=d>1$であるなれば，
解の個数はnを法としてd個である．

定理m7（中国剰余の定理）

$n_1,\cdots,n_s$を１より大きい整数とし，$(n_i,n_j)=1(i\neq j)$とする．
このとき，任意の整数の組$a_1,\cdots,a_s$に対して連立合同式
$x\equiv a_1(\mathrm{mod}\,n_1),\cdots,x\equiv a_s(\mathrm{mod}\,n_s)$
は，$n=n_1,\cdots,n_s$を法として唯1つの解をもつ．

最大公約数，最小公倍数

- 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

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

としても最大公約数は変わらない.

$$(a,b)=g,[a,b]=l$$

$$a,b=gl$$

13
3
1
1

合同式

5^{1221}を14で割った余り

131^{131}を7で割った余り

123^{123}を14で割った余り

7^{2012}を10で割った余り