§3. 合同式

ここでは、m を法とする合同 $\equiv \pmod m$ の概念を学ぶ。$\equiv \pmod m$ を含んだ計算方法に慣れることが目標である。

● 3 - 1 : m を法とする合同

m を自然数とする。2 つの整数 a, b について、$a-b$ が m の倍数であるとき、すなわち、$a-b=qm$ となる整数 q が存在するとき、

$$a \equiv b \pmod m$$

と書いて、a は b に m **を法として合同** (congruent modulo m) であるという。$\bmod m$ は「モジュロ m」または「モッド m」などと読む。a が b に m を法として合同でないことを $a \not\equiv b \pmod m$ で表わす。例えば、$100 \equiv 0 \pmod 2$ であるが、$100 \not\equiv 0 \pmod 3$ である。

整数 a, b が等しい $(a=b)$ ことは a が b に「0 を法として合同」であることと解釈することができるので、「$\equiv \pmod m$」は等号の拡張概念と思うことができる。

● 3 - 2 : 合同式の基本的性質

$m \in \mathbb{N}$ とする。“$\equiv \pmod m$”は以下の 3 つの補題で述べられる性質を持っている。

補題 3 - 2 - 1

$a, b, c \in \mathbb{Z}$ に対して、次が成り立つ。

(i) (**反射律**) $a \equiv a \pmod m$.

(ii) (**対称律**) $a \equiv b \pmod m \quad \Rightarrow \quad b \equiv a \pmod m$.

(iii) (**推移律**) $a \equiv b \pmod m,\ b \equiv c \pmod m \quad \Rightarrow \quad a \equiv c \pmod m$.

(**証明**)

(i) $a-a=0$ は m の倍数であるから、$a \equiv a \pmod m$ が成り立つ。

(ii) $a \equiv b \pmod m$ であると仮定すると、$a-b=qm$ となる $q \in \mathbb{Z}$ が存在する。このとき、$b-a=-qm=(-q)m$ と書けて、$-q \in \mathbb{Z}$ であるから、$b \equiv a \pmod m$ となる。

(iii) $a \equiv b \pmod m$ かつ $b \equiv c \pmod m$ と仮定する。すると、$a-b=q_1 m,\ b-c=q_2 m$ となる $q_1, q_2 \in \mathbb{Z}$ が存在する。このとき、

$$a-c=(a-b)+(b-c)=q_1 m+q_2 m=(q_1+q_2)m$$

と書けて、$q_1+q_2 \in \mathbb{Z}$ であるから $a \equiv c \pmod m$ となる。 □

補題 3 - 2 - 2

$a, b, a', b' \in \mathbb{Z}$ が $a \equiv a' \pmod m$, $b \equiv b' \pmod m$ を満たすとき、次が成り立つ。

(i) $a+b \equiv a'+b' \pmod m$.

(ii) $a-b \equiv a'-b' \pmod m$.

(iii) $ab \equiv a'b' \pmod m$.

(**証明**)

ここでは (i) だけを示し、残りは演習問題とする。$a \equiv a' \pmod m$, $b \equiv b' \pmod m$ なので、$a-a'=q_1 m,\ b-b'=q_2 m$ となる $q_1, q_2 \in \mathbb{Z}$ が存在する。このとき、

$$(a+b)-(a'+b')=(a-a')+(b-b')=(q_1+q_2)m$$

と書けるが、$q_1+q_2 \in \mathbb{Z}$ であるから、$a+b \equiv a'+b' \pmod m$ が成り立つ。 □

演習 3-1* 上の補題の (ii), (iii) を証明せよ。

演習 3-2 $11 \times 13 \times 19 \times 23 + 29 \times 31 \times 37$ を 7 で割ったときの余りを求めよ。

補題 3-2-3
$m \in \mathbb{N},\ a, b, c \in \mathbb{Z}$ とする。$\gcd(c, m) = 1$ のとき、

$$ca \equiv cb \pmod{m} \quad \Rightarrow \quad a \equiv b \pmod{m}.$$

(**証明**)
$ca \equiv cb \pmod{m}$ ならば $m | c(a-b)$ である。$\gcd(c, m) = 1$ なので、[系 1-3-3(1)] により、$m | (a-b)$ となる。故に、$a \equiv b \pmod{m}$ が成り立つ。 □

● 3-3 : 剰余と合同式

m を自然数とする。除法の原理により、任意の整数 a に対して

$$a = qm + r \quad (0 \leq m < r)$$

となる整数 q, r が存在する。このとき、$a \equiv r \pmod{m}$ が成り立つ。r の取りうる値は $0, 1, \ldots, m-1$ のいずれかなので、次が成り立つ。

補題 3-3-1
$m \in \mathbb{N}$ とする。任意の整数は $0, 1, \ldots, m-1$ のいずれかと m を法として合同である。

例 3-3-2 任意の整数は 6 を法とすると、$0, 1, 2, 3, 4, 5$ のいずれかに合同である。例えば、

$$-8 = (-6) + (-2) \equiv -2 \equiv 4 \pmod{6}$$

である。 □

演習 3-3 7 を法とするとき、$-12,\ -1,\ 21,\ 31$ はそれぞれ $0, 1, 2, 3, 4, 5, 6$ のどれと合同になるか。

● 3-4 : 1 次の合同方程式

m を 2 以上の整数とし、X を不定元とする整数係数の 1 次式

$$aX + b \quad (\text{但し、} m \nmid a)$$

を考える。整数 x が $ax + b \equiv 0 \pmod{m}$ を満たすとき、x は**合同方程式** $aX + b \equiv 0 \pmod{m}$ の解である、あるいは、合同方程式 $aX \equiv -b \pmod{m}$ の解である、という。整数 x が合同方程式 $aX + b \equiv 0 \pmod{m}$ の解であるとき、$x \equiv x' \pmod{m}$ を満たすすべての整数 x' も解になる。合同方程式 $aX + b \equiv 0 \pmod{m}$ の解を、m を法としてすべて求めることを、合同方程式 $aX + b \equiv 0 \pmod{m}$ を解くという。m が小さい場合には、X に $0, 1, 2, \cdots, m-1$ を 1 つ 1 つ代入して合同方程式を解くことができる。

例 3-4-1 代入計算により、$x = 0, 1, 2, 3, 4, 5$ の中で $4x \equiv 2 \pmod{6}$ を満たすものは $x = 2, 5$ だけであることがわかる。よって、合同方程式 $4X \equiv 2 \pmod{6}$ の解は 2 と 5 である。 □

● 3-5 : 合同方程式の解の存在条件

合同方程式 $aX \equiv b \pmod{m}$ の解の存在は次の定理を使って直ちに知ることができる。

定理 3 - 5 - 1
m を 2 以上の整数、a を $m \nmid a$ を満たす整数、b を任意の整数とし、$d = \gcd(a, m)$ とおく。このとき、合同方程式 $aX \equiv b \pmod{m}$ の解が存在するための必要十分条件は $d|b$ である。

(**証明**)

I. 合同方程式 $aX \equiv b \pmod{m}$ は解を持つと仮定する。$x \in \mathbb{Z}$ をその解とすると、$b = ax + qm$ となる $q \in \mathbb{Z}$ が存在する。d は a と m の最大公約数だから、$d|a$ かつ $d|m$ であり、したがって、$d|(ax + qm)$ となる。これで、$d|b$ が示された。

Ⅱ. $d|b$ であると仮定し、$b = cd$ $(c \in \mathbb{Z})$ と書く。[系 1 - 3 - 2] により、$ax + my = d$ を満たす $x, y \in \mathbb{Z}$ が存在する。両辺を c 倍して、$cax + cmy = cd = b$ を得る。これより、$a(cx) \equiv b \pmod{m}$ がわかるから、合同方程式 $aX \equiv b \pmod{m}$ は解 $cx \in \mathbb{Z}$ を持つ。 □

上の定理から次の系が導かれる (この系は [系 1 - 3 - 2] を使って直接導くこともできる)。

系 3 - 5 - 2
m を 2 以上の整数、a を任意の整数とするとき、

$$ax \equiv 1 \pmod{m} \text{ となる } x \in \mathbb{Z} \text{ が存在する} \iff \gcd(a, m) = 1.$$

注意 3 - 5 - 3 $\gcd(a, m) = 1$ のとき、$ax \equiv 1 \pmod{m}$ を満たす $x \in \mathbb{Z}$ は m を法として唯一である。なぜなら、$x' \in \mathbb{Z}$ も $ax' \equiv 1 \pmod{m}$ を満たしていたとすると、

$$x' = 1 \cdot x' \equiv (ax)x' = x(ax') \equiv x \cdot 1 = x \pmod{m}$$

となるためである。 □

例 3 - 5 - 4 合同方程式 $2X \equiv 1 \pmod{14}$ は、$\gcd(2, 14) = 2 \neq 1$ だから、解を持たない。他方、合同方程式 $3X \equiv 1 \pmod{14}$ は、$\gcd(3, 14) = 1$ だから、解を持つ。実際、$X = 5$ がその解である。 □

● 3 - 6 : 合同方程式の解き方

m を 2 以上の整数、a を $m \nmid a$ を満たす整数、b を任意の整数とし、$d = \gcd(a, m)$ とおく。[定理 3 - 5 - 1] により、$d|b$ ならば合同方程式 $aX \equiv b \pmod{m}$ は解を持つ。

$$aX \equiv b \pmod{m} \iff \exists Y \in \mathbb{Z} \text{ s.t. } aX - b = mY$$

なので、合同方程式 $aX \equiv b \pmod{m}$ を解くには、X, Y についての不定方程式 $aX - mY = b$ を解けばよい。これは、ユークリッドの互除法を使えば解ける。

演習 3 - 4 合同方程式 $36X \equiv 32 \pmod{100}$ を解け。

合同方程式 $aX \equiv b \pmod{m}$ はまた次のようにして解くこともできる。まず、

$$a = da', \quad m = dm', \quad b = db' \quad (a', m', b' \in \mathbb{Z})$$

とおく。すると、与えられた合同方程式を解くことと合同方程式 $a'X \equiv b' \pmod{m'}$ を解くことは同値となる (但し、合同方程式 $aX \equiv b \pmod{m}$ の解を求めるには、合同方程式 $a'X \equiv b' \pmod{m'}$ の解を m を法として考える必要がある)。$\gcd(a', m') = 1$ なので、[系 3 -

5 -2] と [注意 3 -5 -3] により、$a'x \equiv 1 \pmod{m'}$ を満たす $x \in \mathbb{Z}$ が唯一存在する。このような x を m' を法として求めれば、合同方程式 $a'X \equiv b' \pmod{m'}$ の解は

$$X \equiv xb' \pmod{m'}$$

によって求めることができる。つまり、合同方程式 $aX \equiv b \pmod{m}$ を解くことは、合同方程式 $a'X \equiv 1 \pmod{m'}$ を解くことに帰着される。

例 3 -6 -1 合同方程式 $18X \equiv 2 \pmod{32}$ を解く。

上の合同方程式を解くことは、合同方程式

(3 -6 a) $$9X \equiv 1 \pmod{16}$$

を 32 を法として解くことと同値である。まず、(3 -6 a) を 16 を法として解こう。そのためには、不定方程式 $9X - 16Y = 1$ を解けばよい。この不定方程式の 1 組の解は、ユークリッドの互除法により、$(X, Y) = (-7, -4)$ であることがわかる。よって、合同方程式 $9X \equiv 1 \pmod{16}$ の解は、$X = -7 \equiv 9 \pmod{16}$ である。

したがって、合同方程式 $18X \equiv 2 \pmod{32}$ の解は、32 を法として、9 と $9 + 16 = 25$ の 2 つである。 □