一次合同式

1.　一次合同式の解法

1.1　係数と法が互いに素な場合

まず最初に、整数 q を法とする一次合同式

$$ax \equiv b \bmod q \tag{1}$$

において、$(a, q) = 1$ の場合を考える。

このとき、拡張ユークリッドの互除法を用いると、

$$as \equiv 1 \bmod q$$

となる整数 s を求めることができる。この s を式 (1) の両辺に乗ずることにより、解 x を

$$x \equiv sb \bmod q$$

と求めることができる。

1.2　一般の場合

次に、一般の一次合同式：

$$ax \equiv b \bmod q \tag{2}$$

を考える。このとき、式 (2) が解を持つ必要十分条件は、$d = (a, q)$ が b を割りきることである。また、このとき、解の個数は d 個になる。

このことは、$d = (a, q)$ より、$a = a'd$、$q = q'd$ とおくと、式 (2) は合同式の定義に従って、

$$a'dx - b = q'dt \; (t \in \mathcal{Z}) \tag{3}$$

と書けるから、$d|b$ でなければ解を持たないことは明らかであろう。$d|b$ であるときは、$b = b'd$ とおけるから、式 (3) の両辺を d で割ることにより、

$$a'x \equiv b' \bmod q'$$

を得る。この式では $(a', q') = 1$ であるから、式 (1) の場合であり、解 $x = x_0$ を $0 < x_0 < q'$ で一意に求めることができる。ここで、$x = x_0 + q's (s \in \mathcal{Z})$ とおくと、この x は式 (3) を満たすので、式 (2) の解である。

解の個数が d 個であることは、$x_0 + q's$ と $x_0 + q's'$ が $s \equiv s' \bmod d$ であるときに法 q のもとで合同になることから導かれる。

1.3　具体例

具体例として、

$$24x \equiv 15 \bmod 57 \tag{4}$$

を解いてみよう。

$d = (24, 57) = 3$ であり、$3|15$ であるので解は存在する。式 (4) の $24, 15, 57$ をそれぞれ $d = 3$ で割って、

$$8x \equiv 5 \bmod 19 \tag{5}$$

を得る。拡張ユークリッドの互除法を用いると、$12 \times 8 \equiv 1 \bmod 19$ となるから、式 (5) の両辺に 12 を乗じて、

$$x \equiv 3 \bmod 19$$

を得る。従って、式 (4) の解は、

$$x = 3 + 19s \; (s = 0, 1, 2)$$

と表される。実際に、$x = 3, 22, 41$ が式 (4) を満たし、他に解がないことは容易に確認できる。

2.　連立一次合同式

次に、連立一次合同式：

$$\begin{cases} x \equiv a_1 \bmod q_1 \\ x \equiv a_2 \bmod q_2 \\ \cdots \\ x \equiv a_m \bmod q_m \end{cases} \tag{6}$$

を考える。もちろん、各式は、式 (2) の形であってもよいが、その場合は、1. で述べた方法で上

記の形に直せばよい。式 (6) は、法 $q_1, q_2, \ldots, q_m$ が互いに素（どの 2 つをとっても互いに素ということ）であるときに、$q = q_1 q_2 \cdots q_m$ を法としてただ一つの解を持つ[1]。もし、x' と x'' が解であるとすると、式 (6) において、

$$x' \equiv x'' \equiv a_i \bmod q_i \ (i = 1, 2, \ldots, m)$$

であるので、$x' - x''$ は、各 $q_i (i = 1, 2, \ldots, m)$ の倍数になる。従って、$x' - x''$ は、$q = q_1 q_2 \cdots q_m$ の倍数となるので、結局 $x' \equiv x'' \bmod q$ であることがわかる。

式 (6) を解くために、$Q_1, Q_2, \cdots, Q_m$ を次式を満たすように決める。

$$q = q_1 Q_1 = q_2 Q_2 = \cdots = q_m Q_m$$

次に、

$$Q_i t_i \equiv 1 \bmod q_i \ (i = 1, 2, \ldots, m) \tag{7}$$

を各々解いて $t_i (i = 1, 2, \ldots, m)$ を求める ($(Q_i, q_i) = 1$ であるので必ず解くことができる)。

これらを用いて、式 (6) の解は、

$$x \equiv a_1 Q_1 t_1 + a_2 Q_2 t_2 + \ldots + a_m Q_m t_m \bmod q \tag{8}$$

と表すことができる。これが解であることは、式 (8) を式 (6) の各式に代入することにより確かめられる。実際、

$$Q_i \equiv 0 \bmod q_j \text{ for } i \neq j$$

であるので、

$$a_1 Q_1 t_1 + a_2 Q_2 t_2 + \ldots + a_m Q_m t_m \equiv a_i \bmod q_i$$

となることがわかる。

2.1 具体例

具体例として、以下の問題を解いてみよう。

$$\begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 3 \bmod 5 \\ x \equiv 2 \bmod 7 \end{cases} \tag{9}$$

[1] この条件を満たさなくても解を持つことはある。

法 $3, 5, 7$ は互いに素であるので、式 (9) は $q = 3 \times 5 \times 7 = 105$ を法として解を持つ。

$$Q_1 = 35, Q_2 = 21, Q_3 = 15$$

であるので、

$$\begin{aligned} 35t_1 &\equiv 1 \bmod 3 \\ 21t_2 &\equiv 1 \bmod 5 \\ 15t_3 &\equiv 1 \bmod 7 \end{aligned}$$

を各々解いて、$t_1 = 2$、$t_2 = 1$、$t_3 = 1$ を得る。従って、解 x は、

$$x \equiv 2\times35\times2+3\times21\times1+2\times15\times1 \equiv 23 \bmod 105$$

と求められる。

2.2 一般の合同式の場合

整数係数の多項式 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ について合同式 $f(x) \equiv 0$ を法 $n = pq$(p、q は素数) のもとで考えるとき、以下の定理が成り立つ。

定理 4 p、q が素数であるとき、$n = pq$ とすると、

$$f(x) \equiv 0 \bmod n \tag{10}$$

と、連立合同式

$$\begin{cases} f(x) \equiv 0 \bmod p \\ f(x) \equiv 0 \bmod q \end{cases} \tag{11}$$

は同値である。 □

(証明) 式 *(10)* を満たす解を x_0 とすると、定義より $pq | f(x_0)$ であるので、$p | f(x_0)$ かつ $q | f(x_0)$ となり、式 *(11)* を満たす。逆に、式 *(11)* を満たす $f(x)$ は、p の倍数かつ q の倍数であるので $f(x)$ は $n = pq$ の倍数であることになり、式 *(10)* を満たす。 *Q.E.D.*

一般に、合成数 n を法とする合同式を解くとき、式 (11) のように n の素因数を法とする連立合同式を解く方が効率的である。