等差数列の共通項と中国の剰余の定理

平成 28 年 1 月
富山県教育委員会小中学校課
児童生徒育成係　主幹
片山　喜美

以下のような問題を考える。

問題
$\{a_n\}$ を初項 1 公差 6 の等差数列、$\{b_n\}$ を初項 2 公差 7 の等差数列、$\{c_n\}$ を初項 5 公差 19 の等差数列とする。$\{a_n\}, \{b_n\}, \{c_n\}$　全てに共通な項の一般項を求めよ。

1　便利な数を３つ見つける解法

$a_n \equiv 1 \pmod 6$,　$b_n \equiv 2 \pmod 7$,　$c_n \equiv 5 \pmod{19}$ という観点で考える。
すると、共通項は、連立合同方程式 $a \equiv 1 \pmod 6$,　$a \equiv 2 \pmod 7$,　$a \equiv 5 \pmod{19}$ を満たす数であると言える。

- mod 6 で 1、mod 7, mod 19 で 0 となる数 l_1
- mod 7 で 1、mod 6, mod 19 で 0 となる数 l_2
- mod 19 で 1、mod 6, mod 7 で 0 となる数 l_3

があったとする。このとき、$\{a_n\}, \{b_n\}, \{c_n\}$ の初項 1, 2, 5 をそれぞれ l_1, l_2, l_3 にかけたものを加えて、$a = 1 \cdot l_1 + 2 \cdot l_2 + 5 \cdot l_3$ とすると。

- $a \equiv 1 \cdot 1 + 2 \cdot 0 + 5 \cdot 0 \equiv 1 \pmod 6$
- $a \equiv 1 \cdot 0 + 2 \cdot 1 + 5 \cdot 0 \equiv 2 \pmod 7$
- $a \equiv 1 \cdot 0 + 2 \cdot 1 + 5 \cdot 5 \equiv 5 \pmod{19}$

とあるので、a は、$\{a_n\}, \{b_n\}, \{c_n\}$ に共通な項もしくは、それを負の方向に伸ばしたところにある数になる。
さて、うまく l_1, l_2, l_3 を見つけられるだろうか？

- $l_1 \equiv 0 \pmod 7$ かつ $l_1 \equiv 0 \pmod{19}$ より、l_1 は $7 \times 19 = 133$ の倍数である。
  6, 133 でユークリッドの互除法を行う。

$$
\begin{array}{rrr}
 & 6 & 133 \\
22) & & 132 \\
\hline
 & & 1
\end{array}
\qquad
\begin{array}{rr}
22 & -1
\end{array}
$$

従って、
$6 \cdot (-22) + 133 \cdot 1 = 1$
この式から、
$l_1 = 133 \cdot 1 = 133$

- l_2 については、7 と $6 \times 19 = 114$ で考える。

	7	114
16)		112
	7	2
	6	(3
	1	

49	−3
−48	
1	−3

従って、
$7 \cdot 49 + 114 \cdot (-3) = 1$
この式から、
$l_2 = 114 \cdot (-3) = -342$

- l_3 については、19 と $6 \times 7 = 42$ で考える。

	19	42
2)		38
	19	4
	16	(4
	3	4
1)		3
		1

−11	5
10	
−1	5
	−4
−1	1

従って、
$19 \cdot (-11) + 42 \cdot 5 = 1$
この式から、
$l_3 = 42 \cdot 5 = 210$

以上により、うまく $l_1., l_2, l_3$ が求められる。
$a = 1 \cdot l_1 + 2 \cdot l_2 + 5 \cdot l_3 = 1 \cdot 133 + 2 \cdot (-342) + 5 \cdot 210 = 133 - 684 + 1050 = 499$
$\{a_n\}, \{b_n\}, \{c_n\}$ の公差 $6, 7, 19$ は互いに素であるから、共通項は等差数列になり、その公差はその最小公倍数 $6 \times 7 \times 19 = 798$ である。したがって、上記の 499 は共通項の最小項である。
一般項は , $499 + 798(n-1) = \underline{798n - 299}$

注意 l_1, l_2, l_3 は「正規直交ベクトル」と似ている。
$\vec{e_1} = (1,0,0), \vec{e_2} = (0,1,0), \vec{e_3} = (0,0,1)$ とし、
$\vec{a} = \vec{e_1} + 2\vec{e_2} + 5\vec{e_3}$ とすると、

- $\vec{a} \cdot \vec{e_1} = \vec{e_1} \cdot \vec{e_1} + 2\vec{e_2} \cdot \vec{e_1} + 5\vec{e_3} \cdot \vec{e_1} = 1 \cdot 1 + 2 \cdot 0 + 5 \cdot 0 = 1$
- $\vec{a} \cdot \vec{e_2} = \vec{e_1} \cdot \vec{e_2} + 2\vec{e_2} \cdot \vec{e_2} + 5\vec{e_3} \cdot \vec{e_2} = 1 \cdot 0 + 2 \cdot 1 + 5 \cdot 0 = 2$
- $\vec{a} \cdot \vec{e_3} = \vec{e_1} \cdot \vec{e_3} + 2\vec{e_2} \cdot \vec{e_3} + 5\vec{e_3} \cdot \vec{e_3} = 1 \cdot 0 + 2 \cdot 0 + 5 \cdot 1 = 5$

2　中国の剰余の定理 (Chinese Remainder Theorem)

以下、「数論への出発」(日本評論社)　による。
中国の 1 世紀頃の書「孫子算経」中に、”3 で割れば 2 が余り、5 で割れば 3 が余り、7 で割れば 2 が余るような数は何か ?” という問題と解法が載っているとのことである。

- $3 \times 12 + (5 \cdot 7) \times (-1) = 1$ より、 $l_1 = -35$

- $5 \times (-4) + (3 \cdot 7) \times 1 = 1$ より、 $l_2 = 21$
- $7 \times (-2) + (3 \cdot 5) \times 1 = 1$ より、 $l_3 = 15$

は、互除法を用いるまでもなく、ちょっと数を眺めてみれば思いつく。
$a = 2 \times (-35) + 3 \times 21 + 2 \times 15 = -70 + 63 + 30 = 23$
公差は $3 \cdot 5 \cdot 7 = 105$ なので、一般項は、 $23 + 105(n-1) = 105n - 82$

以下に、連立合同方程式に関する一般論を述べておく。

定理 3．1　自然数 m, n の最大公約数を d 、最小公倍数を l とすると、
$x \equiv a \pmod{m}$　かつ　$x \equiv b \pmod{n}$ が解を持つ必要十分条件は、
$a \equiv b \pmod{d}$ である。また、解を持つときは、 l を法としてただ 1 つである。

証明）もし解があれば、$x = a + ms = b + nt \quad (s, t \in \mathbb{Z})$　とできる。
このとき、 $a - b = -ms + nu$ であり、 $d|m$, $d|n$ であるから、 $d| - ms + nt$ 。
よって、$d|a - b$ 。すなわち、 $a \equiv b \pmod{d}$
　逆に、 $a \equiv b \pmod{d}$ の時、$a - b = kd \quad (k \in \mathbb{Z})$ であるが、
$-mv + nw = d$ を満たす整数 v, w があることより、
$a - b = k(-mv + nw) = -mkv + nkw$ 、$a + mkv = b + nkw$ 。
従って、$x = a + mkv = b + nkw$ とおくと、$x \equiv a \pmod{m}$　かつ　$x \equiv b \pmod{n}$
　ここでもし、x_1, x_2 がともにこの連立方程式の解であるとすると、
$x_1 \equiv x_2 \pmod{m}$ かつ $x_1 \equiv x_2 \pmod{n}$ なので、 $x_1 - x_2$ は、 m 及び n で割り切れる。
すなわち、、最小公倍数 l で割り切れる。 よって、解が存在するとき、それは、l を法としてただ 1 つである。(証明終わり)

定理 3．2　$m_1, m_2, \cdots, m_k$ を k 個の互いに素な自然数であるとする。
このとき、連立方程式 $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$, $\cdots$, $x \equiv a_l \pmod{m_k}$, は解をもつ。それは、mod $m_1 \cdot m_2 \cdot \cdots \cdot m_k$ を法としてただ 1 つである。

証明）定理 3．1 を繰り返し適用して証明できる。
　ここでは、等差数列の共通項を求める際などに、実際に数値計算を実施できる以下の証明を与える。
　$M = m_1 \cdot m_2 \cdot \cdots \cdot m_k, \quad M_i = M/m_i$ とおく。
　条件より、 m_i と M_i は互いに素である。
　従って、 $m_i \cdot x_i + M_i \cdot y_i = 1 \quad (i = 1, 2, \cdots, k)$ を満たす整数がある。
　このとき、 $l_i = M_i \cdot y_i$ とおくと、$l_i \equiv 1 \pmod{m_i}, \quad l_i \equiv 0 \pmod{m_j} \, (j \neq i)$
　よって、 $x = a_1 \cdot l_1 + a_2 \cdot l_2 + \cdots + a_k \cdot l_k$ とすると、条件を満たす。(証明終わり)

　この定理が、先に計算した等差数列の共通項を求める計算方法の根拠になる。
　その際には、
　　$m_i \cdot x_i + M_i \cdot y_i = 1 \quad (i = 1, 2, \cdots, l)$
　の解を求める必要があり、互除法から実際に解を導く方法が役立つ。

3　高校で教える解法

一挙に 3 つの等差数列の共通項を求めるのではなく、

(1) $\{a_n\}, \{b_n\}$　に共通な項の一般項を求めよ。

(2) $\{a_n\}, \{b_n\}, \{c_n\}$　全てに共通な項の一般項を求めよ。

というように、段階的に求めていくのだろう。

3.1　解法 1　数を並べて最小共通項を見つける方法

(1) a_n　:　$1, 7, 13, 19, 25, 31, \underline{37}, 43, \cdots$
b_n　:　$2, 9, 16, 23, 30, \underline{37}, 44, \cdots$
であるから、最小共通項は 37 である。そして、次の共通項までは $\{a_n\}$ で考えると 6 の倍数の差があるし、$\{b_n\}$ で考えると 7 の倍数の差があるので、6, 7 の最小公倍数 42 の差がある。
　従って、一般項は $37 + 42(n-1) = \underline{42n - 5}$

(2) $\{42n-5\}$ と $\{c_n\}$ の共通項を求めればよい。

$42n-5$　:　37, 79, 121, 163, 205, 247, 289, 331, 373, 415, 457, $\underline{499}$, $\cdots$
c_n　:　5, 24, 43, 62, 81, 100, 119, 138, 157, 176, 195, 214, 233, 252,
271, 290, 309, 328, 347, 366, 385, 404, 423, 442, 461, 480, $\underline{499}$, $\cdots$

従って、共通項の初項は 499。また、42 と 19 は互いに素であるから、その最小公倍数は、 $42 \times 19 = 798$ である。
一般項は、　$499 + 798(n-1) = \underline{798n - 299}$

3.2　解法 2　$a_k = b_l$ の式変形をうまく用いる方法

(1) $a_k = b_l$ とすると、 $1 + 6(k-1) = 2 + 7(l-1)$,　$6k - 5 = 7l - 5$,　$6k = 7l$
最後の式で左辺は 6 で割り切れるから、右辺の $7l$ も 6 で割り切れなければならないが、6 と 7 は互いに素であるから、l が 7 で割り切れなければならない。よって、$l = 6n$ とできる。$6k = 7 \cdot 6n$ だから、$k = 7n$ 。
共通項は a_k に代入して、 $6 \cdot 7n - 5 = \underline{42n - 5}$

(2) $\{42n-5\}$ と $\{c_n\}$ の共通項を求める。
$42k-5 = 4+19(l-1)$ とおく。$42k = 19l-9$ として、両辺から 42 の倍数を引いていき、右辺が 19 でくくれるようになればよい。なかなか手間取るので、 mod 19 で考える。
$42 \equiv 4 \pmod{19}$ なので、右辺の -9 から順に引いて、-13, -17, -2, -6, -10, -14, -18, -3, -7, -11, -15, 0。
すなわち、12 回引いて 0 に合同となるから、

$42k - 42 \times 12 = (19l - 9) - 42 \times 12, \quad 42(k - 12) = 19(l - 27)$
42 と 19 が互いに素であることから、この両辺を $= 42 \cdot 19(n - 1)$ とおける。
$k - 12 = 19(n - 1)$ なので、
$42k - 5 = 42\{\cdot 19(n - 1) + 12\} - 5 = 499 + 798(n - 1) = \underline{798n - 299}$

注意 大きな数になると、互除法の手数がかかる場合がある。冒頭の問題は、平成 28 年 1 月に周囲の人に「頭の体操」として考えてもらったものであるが、さらに「初項 4、公差 23 の等差数列 $\{d_n\}$ 」を加えて、4 つの等差数列の共通項を求めてもらう問題も出していた。互除法を筆算でやっていたが、大きな数を扱うこともあり、解答例を作成するついでに、エクセルで計算するものを簡単な VBA で作成した。

それを周囲にメールで送ったいたら、ちょうど 2016 年センター試験に「92x+197y=1 の整数解」が出題された。