数理パズルから数学の世界へ（１）

林　　雄一郎*

１　はじめに

数理パズルにはハッとするような面白いものがあり、その中には美しい数理が潜んでいて数学教育上効果的なものが少なくない。

このようなパズルを解くうちに数や図形に関心を深め、基本的な原理・法則を学び、体系的に組み立てていく数学の考え方を体得し、事象を数学的に翻訳し解決する力が培われれば好ましいと思う。本稿では、以上の観点から中国剰余定理にちなんだパズルを紹介する。

２　問題とその解法

> ２１世紀（２００１年～２１００年）の中で、３，５，７で割った余りがそれぞれ１，４，３である年は西暦何年か？(1)

（解１）

高校生が解くとすれば、求める数を$x=3s+1=5t+4=7u+3$とおき

$3(s-1)=5t \quad s=5s'+1 \quad \therefore x=15s'+4$　他方、$15s'+4=7u+3$

$15(s'+1)=7(u+2) \quad s'+1=7s'' \quad s'=7s''-1 \quad \therefore x=15(7s''-1)+4=105s''-11$

$2001\le 105s''-11\le 2100 \quad 19.7\cdots\le s''\le 20.1\cdots$

$\therefore s''=20 \quad x=105\times 20-11=2089$（年）　というものであろう。

（解２）

合同式を学んだ大学生なら次のような解き方をするだろう。

$x\equiv 1(\mathrm{mod}3), x\equiv 4(\mathrm{mod}5), x\equiv 3(\mathrm{mod}7) \quad x=1+3s \quad 1+3s\equiv 4(\mathrm{mod}5) \quad s\equiv 1(\mathrm{mod}5)$

$3s\equiv 3(\mathrm{mod}15) \quad x=1+3s=1+(3+15s')=4+15s'\equiv 3(\mathrm{mod}7) \quad 14s'+s'\equiv -1(\mathrm{mod}7)$

$s'\equiv -1(\mathrm{mod}7) \quad s'=-1+7s'' \quad \therefore x=4+15s'=4+15(-1+7s'')=-11+105s''$

＊北海道情報大学

後は高校生の解と同様。

（解３）

数学者ならばこの問題は次のように解く[(1)]。

一般に、３，５，７で割って余りがa,b,cとなる整数の一般形は次式となる。

$70a+21b+15c+105t$　tは整数　…… (＊)

この式で　$a=1,b=4,c=3$　を代入する　　$70\times1+21\times4+15\times3+105t=199+105t$

$2001\le199+105t\le2100$　$t=18$　よって求める答えは　$199+105\times18=2089$(年)

何故（＊）式が成り立つかということから数学の世界が始まる。

３，５，７で割って余りがそれぞれ１，４，３となる数の集合をWとおく。

Wの特殊解をx_0とすれば一般解xは次式で表される。

$x-x_0\equiv0(\mathrm{mod}105)$　よって　　$W=\{x_0+105t\,|\,t\in Z\}$となる。

そこでx_0を見付けねばならない。それには頭ごなしだが次式を考える。

$70\equiv1(\mathrm{mod}3),70\equiv0(\mathrm{mod}5),70\equiv0(\mathrm{mod}7)$

$21\equiv0(\mathrm{mod}3),21\equiv1(\mathrm{mod}5),21\equiv0(\mathrm{mod}7)$

$15\equiv0(\mathrm{mod}3),15\equiv0(\mathrm{mod}5),15\equiv1(\mathrm{mod}7)$

各行にa,b,cを掛ける。

$70a\equiv a(\mathrm{mod}3),70a\equiv0(\mathrm{mod}5),70a\equiv0(\mathrm{mod}7)$

$21b\equiv0(\mathrm{mod}3),21b\equiv b(\mathrm{mod}5),21b\equiv0(\mathrm{mod}7)$

$15c\equiv0(\mathrm{mod}3),15c\equiv0(\mathrm{mod}5),15c\equiv c(\mathrm{mod}7)$

列ごとに和を取る。

$70a+21b+15c\equiv a(\mathrm{mod}3),70a+21b+15c\equiv b(\mathrm{mod}5),70a+21b+15c\equiv c(\mathrm{mod}7)$

したがって、$70a+21b+15c\in W$　となる。これが特殊解x_0である。

なお、数式処理システム mathematica にはこの特殊解を求める数論的関数があり、ChineseRemainder[{1, 4, 3}, {3, 5, 7}]で非負最小整数 94 (=-11+105×1) が得られる。

以上の考え方を一般化したものが次の定理である。

定理

$m_1,m_2,\cdots,m_k$が２つずつ互いに素で、$a_1,a_2,\cdots,a_k$は任意の整数とするとき

$x\equiv a_1(\mathrm{mod}\,m_1),x\equiv a_2(\mathrm{mod}\,m_2),\cdots,x\equiv a_k(\mathrm{mod}\,m_k)$を満足させる$x_0$は$M\equiv m_1m_2\cdots m_k$

を法として唯一つ存在する。一般解は　$x \equiv x_0 \pmod{M}$　　$x = x_0 + Mt$　$t \in Z$

定理の証明は次の通りである[1][2]。

$M = m_1 m_2 \cdots m_k$　$M_i = M / m_i$　とおくと　$(m_i, M_i) = 1$　だから

1次不定方程式　$m_i s_i + M_i t_i = 1$　は整数解s_i, t_iをもつ。$\therefore M_i t_i \equiv 1 \pmod{m_i}$

$(M_i t_i) a_i \equiv a_i \pmod{m_i}$　$i \neq j$ならば$m_j \mid M_i$　より$M_i t_i \equiv 0 \pmod{m_j}$

$(M_i t_i) a_i \equiv 0 \pmod{m_j}$　$M_i t_i$は70,21,15に当たる。

これから　$\sum_{i=1}^{k} (M_i t_i) a_i$が特殊解になる。一般解は、特殊解に$Mt$を加えた形になる。

この定理は中国剰余定理（Chinese Remainder Theorem、この名称はレオナード・E・ディクソンによる[3]という）と呼ばれ、中国の算術書「孫子算経」（3～5世紀）に記されていたものである。

それには、「今、物があるが数は不明である。三つずつ数えると二余り、五で割ると三余る。七で割ると二余る。その数如何？」と記され答は二十三とある。

この解法として、「三で割ると二余る数として百四十（$70a = 70 \times 2$）と置く。五で割ると三余る数として六十三（$21b = 21 \times 3$）と置く。七で割ると二余る数として三十（$15c = 15 \times 2$）と置く。これらを足し合わせて、二百三十三（$70a + 21b + 15c = 233$）これから二百十（105×2）を引いて答を得る。一般に、三つずつ数えて一余ると、その度に七十と置く。五で割った余りに二十一をかける。七で割った余りに十五をかける。百六以上なら百五を引くことで答を得る」とある。もっとも、$x = 23 + 105t$（$t \in Z$）はすべて解なのだから、105を引かなくても128,233はこの問題の解なのである。

この問題は日本にも伝えられて「百五減算」（吉田光由：「塵劫記」第十三）として知られている。なお、１３世紀、南宋の秦九韶は１次合同式を拡張されたユークリッド互除法で解くことでこの定理と同等の結果を得たという。その方法を検証してみる。

今、孫子算経の問題は$x \equiv 2 \pmod{3}, x \equiv 3 \pmod{5}, x \equiv 2 \pmod{7}$と１次合同式で表される。ここで３と３５（＝５×７）、５と２１（＝３×７）、７と１５（＝３×５）は互いに素だから$(m, n) = (3,35), (5,21), (7,15)$とおいたとき不定方程式$am + bn = 1$の特殊解は“拡張されたユークリッド互除法”でそれぞれ求められる。例えば、$m = 3, n = 35$

の場合は互除法で　$35=11\times3+2, 3=1\times2+1, 2=2\times1$　となる。これを逆に式変形して不定方程式の特殊解を求めるのが拡張ユークリッド互除法である。

$$1=3-1\times2=3-1\times(35-11\times3)=12\times3+(-1)\times35$$

$\therefore (a,b)=(12,-1)$ は特殊解である。同様にすれば $(m,n)=(5,21),(7,15)$ の場合はそれぞれ特殊解は $(a,b)=(-4,1),(-2,1)$ となる。　$(-4)\times5+1\times21=1, (-2)\times7+1\times15=1$

そこで　$-35\equiv1(\mathrm{mod}3), 21\equiv1(\mathrm{mod}5), 15\equiv1(\mathrm{mod}7)$　となることが分かる。

他方

$$-35\equiv0(\mathrm{mod}5), -35\equiv0(\mathrm{mod}7)$$
$$21\equiv0(\mathrm{mod}3), 21\equiv0(\mathrm{mod}7)$$
$$15\equiv0(\mathrm{mod}3), 15\equiv0(\mathrm{mod}5)$$

すると

$$-35\times2+21\times3+15\times2\equiv1\times2+0\times3+0\times2=2(\mathrm{mod}3)$$
$$-35\times2+21\times3+15\times2\equiv0\times2+1\times3+0\times2=3(\mathrm{mod}5)$$
$$-35\times2+21\times3+15\times2\equiv0\times2+0\times3+1\times2=2(\mathrm{mod}7)$$

したがって、$-35\times2+21\times3+15\times2=23$ は特殊解、一般解は $23+105t$ となる。
以上の方法が秦九韶の方法であろう。これは１９世紀に一宣教師によってヨーロッパに伝えられたという。また、これはガウスの Disquisitiones Arithmaticae（「算術研究」）に述べられた前述の定理の証明の方法と同じである。

3　おわりに

この問題が数理パズルなのか数学の問題なのかは判然としない。パズルと名がつくには見た目にとっつきやすさがなくてはならないのだろう。そういう点ではこの問題はパズルの類なのかもしれないが奥の深い問題である。合同式はそんなに難しいものではないから高校生に教えてはどうか。そうすれば数の性質を考察する際の数学の世界がずいぶん広がるに違いない。

参考文献

（１）　土井幸雄：数とパズルの１８話、日本評論社、2006
（２）　高木貞治：初等整数論講義（第２版）、共立出版、昭和 55 年
（３）　フリー百科事典「ウィキペディア」、http://ja.wikipedia.org/wiki