不定方程式を合同方程式で解く
～合同方程式の教材化をめざして～

仁平（にへい）　政一（まさかず）

§1. はじめに

合同式が発展学習として数学Aの教科書（例えば文献[1，p.128]）に取り上げられていますが，合同式を用いる有用性と面白さを体験できるまでの内容には到っていないように思われます。一次不定方程式の整数解を求める際，合同方程式を用いると容易にしかもただちに解ける場合があります。例えば，文献[1]の例題「不定方程式 $4x+7y=1$ の整数解を求めよ」などがそれにあたります。本稿の目的は合同方程式のもつ魅力とその教育的価値について述べることです。

§2. 合同式の定義とその性質

合同式の定義やその性質については周知のこととは思いますが念のため述べることにします。次の合同式の定義は文献[1，p.128]によります。

m は正の整数とします。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 m で割り切れるとき，a と b は **m を法として合同である**といい，式で

$$a \equiv b \pmod{m}$$

と表します。このような式を**合同式**と言います。

a と b が m を法として合同であることは「a を m で割った余りと b を m で割った余りが等しい」ことと同じになります。なお，「mod」はラテン語の modulus を略記したものです。

以下では，a，b，c，d は整数，m，n，k は自然数とします。このとき，合同式について次に述べるような性質が成り立ちます。

公式1　(1)　$a \equiv a \pmod{m}$
(2)　$a \equiv b \pmod{m}$ のとき　$b \equiv a \pmod{m}$
(3)　$a \equiv b \pmod{m}$，$b \equiv c \pmod{m}$ のとき　$a \equiv c \pmod{m}$

(1)，(2)，(3)はそれぞれ反射律，対称律，推移律と呼ばれています。

公式1から，容易に次を得ることができます。

公式2　$a \equiv c \pmod{m}$，$b \equiv d \pmod{m}$ のとき
(4)　$a+b \equiv c+d \pmod{m}$
(5)　$a-b \equiv c-d \pmod{m}$
(6)　$ab \equiv cd \pmod{m}$
(7)　$a^n \equiv c^n \pmod{m}$

以上の(1)から(7)までの性質は[1]に述べられています。さらに，性質を付け加えておきます。この分については証明も付けておきます。なお，$(a，b)$ は整数 a と b の最大公約数を表します。また，$a|b$ は，a が b を割り切ることを表します。

公式3　c は0でない任意の整数とする。このとき，次が成り立つ。
(8)　$a \equiv b \pmod{m}$ ならば $ca \equiv cb \pmod{m}$
(9)　$a \equiv b \pmod{m}$ ならば $ca \equiv cb \pmod{cm}$

証明　(9)を示す。条件より　$m|a-b$
よって　$cm|c(a-b)$
このことは，$ca \equiv cb \pmod{cm}$ を示している。終

公式4　$ca \equiv cb \pmod{m}$ のとき，次が成り立つ。
(10)　$(c，m)=1$ ならば $a \equiv b \pmod{m}$
(11)　$(c，m)=d\ (>1)$ ならば $a \equiv b \left(\mathrm{mod}\ \dfrac{m}{d}\right)$

証明　(10)　条件より　$m|c(a-b)$
$(c，m)=1$ であるから　$m \nmid c$
よって　$m|a-b$
したがって　$a \equiv b \pmod{m}$

⑾ $(c,\ m)=d$ であるから　$c=dr,\ m=ds$
$(r,\ s\in \boldsymbol{Z})$ と書くことができる。ただし，$\boldsymbol{Z}$ は整数の集合を表します。
このとき，$(c,\ m)=(dr,\ ds)=d$ であるから
$$(r,\ s)=1$$
条件より $m|c(a-b)$ であるから　$m|dr(a-b)$
また，$m=ds$ より　　$ds|dr(a-b)$
よって　　$s|r(a-b)$
$(r,\ s)=1$ であるから　　$s\nmid r$
よって　　$s|a-b$　すなわち　$a\equiv b\pmod{s}$
$s=\dfrac{m}{d}$ であるから求める結果を得る。　終

合同式の性質について一通り述べましたので，いよいよ本題に入ります。

§3. 1次合同方程式の解法と1次不定方程式への応用

最初に合同方程式の定義とその解き方を述べます。

一般に，a は0でなく m で割り切れない整数，b は整数，m は自然数とするとき
$$ax\equiv b\pmod{m}\qquad\cdots\cdots(*)$$
を満たす x の整数値を求めることを**合同式を解く**と言い，このような x の整数値全部を合同式(＊)の**解**と言います。x の次数が1なので合同式(＊)は(**1元)1次合同方程式**と呼ばれています([2])。

ここで，実際に，1次合同方程式
$$3x\equiv 4\pmod{7}$$
を解いてみましょう。

公式3⑻を用いて合同式の両辺を2倍すると
$$6x\equiv 8\equiv 1\pmod{7}\qquad\cdots\cdots①$$
ここで　　$7x\equiv 7\pmod{7}$　　……②
②から①を引くと(公式2⑸を利用)，求める解
$$x\equiv 6\pmod{7}$$
を得ることができます。

それでは，早速1次不定方程式の問題を合同方程式を用いて解いてみましょう。

> **例1**　([1]，p.135)　次の方程式の整数解をすべて求めよ。
> ⑴　$4x+7y=1$　　⑵　$4x-9y=5$

【解答】　⑴　1次合同方程式
$$4x\equiv 1\pmod{7}\qquad\cdots\cdots①$$
を解けば求める整数解が得られることがわかる。
公式3⑻を用いて，①の合同式の両辺を2倍すると
$$8x\equiv 2\pmod{7}\qquad\cdots\cdots②$$
また
$$7x\equiv 0\pmod{7}\qquad\cdots\cdots③$$
②から③を引くと(公式2⑸の性質を利用)
$$x\equiv 2\pmod{7}$$
したがって
$$x=7k+2\quad(k\text{ は整数})$$
これを与式に代入すると
$$y=-4k-1\quad(k\text{ は整数})$$
よって，求める整数解は
$$x=7k+2,\ y=-4k-1\quad(k\text{ は整数})$$
⑵　合同方程式
$$4x\equiv 5\pmod{9}$$
を解けばよい。
この合同式の両辺を2倍すると
$$8x\equiv 10\equiv 1\pmod{9}\qquad\cdots\cdots④$$
また
$$9x\equiv 0\pmod{9}\qquad\cdots\cdots⑤$$
⑤から④を引くと
$$x\equiv -1\pmod{9}$$
よって
$$x=9k-1\quad(k\text{ は整数})$$
これを与式に代入すると
$$y=4k-1\quad(k\text{ は整数})$$
したがって，求める整数解は
$$x=9k-1,\ y=4k-1\quad(k\text{ は整数})$$

合同方程式を用いて解く方法を，通常の方法(教科書の解法)で解いた後，別解として示すことによって，より簡単に解けることを知り，生徒達の合同式への関心を高めることにつながるのではないでしょうか。

次に，合同方程式
$$2x\equiv 5\pmod{6}$$
を考えてみます。$2x-5$ は奇数なので，6で割り切れることはありません。よって解は存在しません。このことからわかるように，1次合同方程式は常に解をもつとは限りません。このことについては次のことが知られています([3]，p.29)。なお，証明は割愛します。

定理 1　1 次合同方程式

$$ax \equiv b \pmod{m}$$

は $d=(a,\ m)$ とするとき，$d=1$ のときは，1 つの解をもち，$d>1$ であるときは，$d \mid b$ のときに限って解をもち，その解の個数は d である。

ここで，念のため $d>1$ の場合の例をあげておきましょう。

例 2　$8x \equiv 2 \pmod{10}$ を解け。

【解答】　$(8,\ 10)=2$ および $2 \mid 2$ であるから，解は存在する。

$$10x \equiv 10 \pmod{10} \quad \cdots\cdots ①$$
$$8x \equiv 2 \pmod{10} \quad \cdots\cdots ②$$

①から②を引くと

$$2x \equiv 8 \pmod{10}$$

ここで，公式 4 (11) を用いると

$$x \equiv 4 \pmod{5}$$

よって，(mod 10) の解は

$$x \equiv 4 \pmod{10},\ x \equiv 9 \pmod{10}$$

の 2 個である。

§4. 連立合同方程式とその応用

ここでは，連立合同方程式の解き方とその応用例について述べます。

早速，例題を通して解き方を示します。

例 3　次の連立合同方程式を解け。

$$\begin{cases} 2x \equiv 3 \pmod{3} \\ x \equiv -1 \pmod{5} \end{cases}$$

【解答】　公式 3 (9) を用いて，法を 15 にそろえると

$$\begin{cases} 10x \equiv 15 \pmod{15} & \cdots\cdots ① \\ 3x \equiv -3 \pmod{15} & \cdots\cdots ② \end{cases}$$

ここで，②の合同式の両辺を 3 倍すると

$$9x \equiv -9 \equiv 6 \pmod{15} \quad \cdots\cdots ③$$

①から③を引くと

$$x \equiv 9 \pmod{15}$$

これは，与式を満たすから求める解である。

注．例 3 については解があるという保証をしていませんので，次々の式の変形が同値変形とは限らないので，解になっているかどうか確かめました。

これで，準備が済んだので応用例の紹介に入ります。

例 4　([1]，p.137)　6 で割ると 1 余り，11 で割ると 5 余るような自然数のうち，3 桁で最小のものを求めよ。

【解答】　題意から次の連立合同式を解けばよいことがわかる。

$$\begin{cases} x \equiv 1 \pmod{6} & \cdots\cdots ① \\ x \equiv 5 \pmod{11} & \cdots\cdots ② \end{cases}$$

公式 3 (9) を用いて，法を 66 にそろえると

$$\begin{cases} 11x \equiv 11 \pmod{66} & \cdots\cdots ③ \\ 6x \equiv 30 \pmod{66} & \cdots\cdots ④ \end{cases}$$

④の合同式の両辺を 2 倍すると

$$12x \equiv 60 \pmod{66} \quad \cdots\cdots ⑤$$

⑤から③を引くと

$$x \equiv 49 \pmod{66}$$

よって

$$x = 66k + 49 \quad (k \text{ は整数})$$

したがって，求める数は $k=1$ の場合で，115 である。

上記の例にしたがって，次の問題もただちに解くことができます。

問　([1]，p.138)　7 で割ると 5 余り，13 で割ると 8 余るような自然数のうち，3 桁で最大のものを求めよ。

これらに関しても，通常の方法(教科書の解法)で解いたのち，別解として与えることにより，教科書の解法に比べて簡明であることを知り，合同式により興味・関心をいだくのではないかと思われます。

もう一つ面白い応用例を紹介しておきましょう。それは**百五減算**として知られている問題です。

例 5　ある数 a は 3 で割ると 1 余り，5 で割ると 2 余り，7 で割ると 3 余る。このとき，a を 105 で割った余りを求めよ。

【解答】　題意から次の連立合同式を解けばよいことがわかる。

$$\begin{cases} a \equiv 1 \pmod{3} & \cdots\cdots ① \\ a \equiv 2 \pmod{5} & \cdots\cdots ② \\ a \equiv 3 \pmod{7} & \cdots\cdots ③ \end{cases}$$

①と②の法を 15 にそろえると

$$\begin{cases} 5a \equiv 5 \pmod{15} & \cdots\cdots ④ \\ 3a \equiv 6 \pmod{15} & \cdots\cdots ⑤ \end{cases}$$

⑤の合同式の両辺を2倍したものから④を引くと

$$a\equiv 7 \pmod{15}$$

次に

$$\begin{cases} a\equiv 7 \pmod{15} \\ a\equiv 3 \pmod{7} \end{cases}$$

を解く。法を105でそろえる。

$$\begin{cases} 7a\equiv 49 \pmod{105} & \cdots\cdots ⑥ \\ 15a\equiv 45 \pmod{105} & \cdots\cdots ⑦ \end{cases}$$

⑥の合同式の両辺を2倍して⑦から引くことにより

$$a\equiv -53\equiv 52 \pmod{105}$$

よって

$$a=105k+52 \quad (k \text{ は整数})$$

したがって，求める数は52である。

最後に，2次，3次合同方程式の話をしておきます。

§5. 高次合同方程式と不定方程式への応用

$f(x)$ は整数を係数とする多項式で，最高次の項の次数が n であって，その係数が m で割り切れないとき

$$f(x)\equiv 0 \pmod{m}$$

を**(1元) n 次合同方程式**と言います。

ここで，簡単な2次，3次の合同方程式の例をあげておきます。

例6　次の合同方程式を解け。
(1)　$4x^2\equiv 1 \pmod 5$　　(2)　$x^3\equiv 4x \pmod 5$

【解答】 (1)　$4x^2-1\equiv 0 \pmod 5$ の左辺の式を因数分解すると，

$$(2x-1)(2x+1)\equiv 0 \pmod 5$$

よって，$2x-1$，$2x+1$ のうちどちらかが5の倍数である。

したがって

$$2x\equiv 1 \pmod 5,\quad 2x\equiv -1\equiv 4 \pmod 5$$

のいずれかが成り立つ。

最初に $2x\equiv 1 \pmod 5$ を解く。

合同式の両辺を2倍すると

$$4x\equiv 2 \pmod 5 \qquad \cdots\cdots ①$$

一方

$$5x\equiv 5 \pmod 5 \qquad \cdots\cdots ②$$

②−①から

$$x\equiv 3 \pmod 5 \qquad \cdots\cdots ③$$

次に，$2x\equiv 4 \pmod 5$ を解く。

$(2,\ 5)=1$ より，公式4⑽を用いると

$$x\equiv 2 \pmod 5 \qquad \cdots\cdots ④$$

逆に，③と④はもとの合同方程式の解である。

したがって，求める解は

$$x\equiv 2 \pmod 5,\quad x\equiv 3 \pmod 5$$

(2)　$x^3-4x\equiv 0 \pmod 5$ の左辺の式を因数分解すると，

$$x(x-2)(x+2)\equiv 0 \pmod 5$$

よって，x，$x-2$，$x+2$ のどれかが5の倍数である。

したがって

$x\equiv 0 \pmod 5$，$x\equiv 2 \pmod 5$，

$x\equiv -2\equiv 3 \pmod 5$

のいずれかが成り立つ。これらはもとの合同式の解である。よって，求める解は

$x\equiv 0 \pmod 5$，$x\equiv 2 \pmod 5$，$x\equiv 3 \pmod 5$

である。

上記の例では2次の合同方程式の解は2個，3次の合同方程式の解は3個でした。このようなことは一般にも成り立つのかと思うのはごく自然なことでしょう。

ところが，合同方程式 $x^2-1\equiv 0 \pmod 8$ の解は1，3，5，7の4個で，これに対して，合同方程式 $x^2-2\equiv 0 \pmod 3$ は解をもちません。

高次合同方程式の解については次の事実が知られています([3]，p.35)。

定理2　素数 p を法とする n 次合同方程式

$$a_0x^n+a_1x^{n-1}+\cdots\cdots+a_n\equiv 0 \pmod p$$

の異なる解はたかだか n 個である。

紙面の関係上証明は割愛しますので，それについては上記の文献([3]，p.35)を参照して下さい。

ここで，応用例を1つ紹介します。

例7　次の不定方程式の整数解をすべて求めよ。

$$x^2+2x+35y=129$$

【解答】　与式は

$$(x+1)^2+35y=130$$

と変形できる。

$x+1=z$ とおくと

$$z^2+35y=130$$

ここで，2次の合同方程式

$$z^2\equiv 130\equiv 25 \pmod{35}$$

を解くと

$z \equiv 5 \pmod{35}$ または $z \equiv -5 \pmod{35}$

$z = x + 1$ より

$x \equiv 4 \pmod{35}$ または $x \equiv -6 \pmod{35}$

したがって

$x = 35k + 4$ （k は整数） または

$x = 35k - 6$ （k は整数）

を得る。

これらを与式に代入すれば，求める整数解

$x = 35k + 4$，$y = -35k^2 - 10k + 3$ （k は整数）；

$x = 35k - 6$，$y = -35k^2 + 10k + 3$ （k は整数）

を得る。

§6. おわりに

限られた授業時数の中では「あれもこれも」というわけにはいきません。

本文中でも述べたように，合同式を用いた解法を別解として示すことにより，それ程時間をかけることなく合同式や合同方程式のもつ便利さや魅力を体感させることができると考えます。

このようなことにより，初等整数論で重要な役割を演じる合同式に興味・関心をいだく生徒が一人でも多く現れるなら教育的価値が十分にあると考えます。

《参考文献》

〔1〕 大島利雄他，数学 A，数研出版（平成 24 年）

〔2〕 芹沢正三，ブルーバックス数論入門―証明を理解しながら学べる―，講談社 (2008)

〔3〕 高木貞治，初等整数論講義（第 2 版），共立出版 (1971)

（元茨城県立藤代高等学校）