合同式に関する教材開発について
～中国式剰余定理を中心に据えて～

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の教科書に取り上げられていますが，その内容は，今のところ合同式の基本性質とそれに関する簡単な例題を紹介するというところで留まっています（例えば文献〔2〕，p.128）。

そこで，本稿の目的は，生徒の興味を引きそうな合同式に関する題材をいくつか紹介することです。

その内容は不定方程式の合同式を用いての解法と中国式剰余定理に関する面白い問題の紹介になります。

§2. 不定方程式の合同式による解法

今年度（平成 28 年度）の大学入試センター試験の数学Ⅰ・数学Aに次のような問題が出題されていました。

問　不定方程式 $92x+197y=1$ を満たす整数 x，y の組の中で，x の絶対値が最小のものは

$x=$ア イ，$y=$ウ エ

である。

不定方程式 $92x+197y=10$ を満たす整数 x，y の組の中で，x の絶対値が最小のものは

$x=$オカキ，$y=$クケ

である。

この問題はユークリッドの互除法を用いて容易に解くことができますが，合同式を用いても，もちろん解くことができます。

例えば次のようにして解くことができます（〔1〕）。

合同式を用いた解法

（前半）$92x+197y=1$ より

$$92x\equiv 1 \pmod{197} \qquad ①$$

①×2 より

$$184x\equiv 2 \pmod{197}$$

ところで　$184x\equiv -13x \pmod{197}$ であるから

$$-13x\equiv 2 \pmod{197} \qquad ②$$

②×7 より

$$-91x\equiv 14 \pmod{197} \qquad ③$$

①＋③ より

$$x\equiv 15 \pmod{197}$$

よって，

$x=15+197k$（k は整数）

と書くことができる。

$|x|$ が最小となるのは，明らかに $k=0$ のときなので　$x=15$，$y=-7$

（後半）$92x+197y=10$ より

$$92x\equiv 10 \pmod{197} \qquad ④$$

④×2 より

$$184x\equiv 20 \pmod{197}$$

ところで，$-197x\equiv 0 \pmod{197}$ であるから

$$-13x\equiv 20 \pmod{197} \qquad ⑤$$

⑤×7 より

$$-91x\equiv 140 \pmod{197} \qquad ⑥$$

④＋⑥ より

$$x\equiv 150\equiv -47 \pmod{197}$$

よって，

$x=-47+197l$（l は整数）

と書くことができる。

$|x|$ が最小となるのは，明らかに $l=0$ のときなので　$x=-47$，$y=22$　□

このように別解として合同式を用いた解法を紹介することで，合同式への興味を持たせることができ，その基本性質の理解をさらに深めることができるのではないだろうか。

次に，中国式剰余定理に関係する問題で面白い教材となり得るものをいくつか紹介しましょう。

§3. 中国式剰余定理とそれに関する問題

早速問題から入りましょう。

問題 1 (1) a は 21 で割ると 8 余る数である。a を 3 で割ったときの余りと 7 で割ったときの余りを求めよ。

(2) b は 3 で割ると 2 余り，7 で割ると 1 余る数である。このとき b を 21 で割ったときの余りを求めよ。

解 (1) 条件より，

$$a=21k+8 \quad (k \text{ は整数})$$

と書くことができる。よって，

$$a=21k+8\equiv 0\cdot k+8\equiv 2 \pmod 3$$
$$a=21k+8\equiv 0\cdot k+8\equiv 1 \pmod 7$$

したがって，a を 3 で割った余りは 2, 7 で割った余りは 1 である。

(2) $b=21k+x$ (k は整数で $0\leqq x\leqq 20$) とおく。

$b\equiv 2 \pmod 3$ より

$$21k+x\equiv 2 \pmod 3 \quad \therefore \quad x\equiv 2 \pmod 3$$

$b\equiv 1 \pmod 7$ より

$$21k+x\equiv 1 \pmod 7 \quad \therefore \quad x\equiv 1 \pmod 7$$

よって，0 から 20 までの数字の中で，3 で割ると 2 余り，7 で割ると 1 余る数を探せばよい。3 で割って 2 余る数は

2, 5, 8, 11, 14, 19

であるから，この中で 7 で割ると 1 余る数は 8。したがって，b を 21 で割った余りは 8 である。□

問題 1 において，(2)の方が(1)より面白い。では，“(2)のような問題は無条件に作れるのだろうか”と思うことは自然に沸き起こる疑問でしょう。

これに対する「答」が「中国式剰余定理」になります。

定理を述べるために，念のため用語の説明をしておきましょう。

Z/pZ (p は自然数) で p 剰余群を表します。例えば，

$$Z/5Z=\{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4}\}$$

となります。$A\times B$ で集合 A と B の直積を表し，記号「≅」は群の同型を意味します。

次に示す定理が中国式剰余定理と呼ばれているもので，2000 年以上前から知られている事実であると言われています ([3], p.60)。なお，証明については文献 ([3], [4]) を参照して下さい。

問題を作成する際に役に立つ定理です。

定理 (中国式剰余定理) m, n は互いに素な自然数とする。このとき，次が成り立つ。

$$Z/mnZ\cong(Z/mZ)\times(Z/nZ)$$

3 と 7 は互いに素ですから

$$Z/21Z\cong(Z/3Z)\times(Z/7Z)$$

より，上記の定理から問題 1 (2)の解の存在が保証されます。

この定理は次のように一般化されます。

n_1, n_2, …, n_k はどの 2 つも互いに素な自然数とする。このとき，

$$Z/n_1n_2\cdots n_kZ\cong(Z/n_1Z)\times(Z/n_2Z)\times\cdots\times(Z/n_kZ)$$

例えば，2, 3, 5 は互いに素ですから

$$Z/30Z\cong(Z/2Z)\times(Z/3Z)\times(Z/5Z) \qquad (*)$$

が成り立ちます。

次に，(*) によって解が保証される問題を考えてみましょう。

§4. 発展問題

問題 2 ある数 a は，2 で割ると 1 余り，3 で割ると 2 余り，5 で割ると 3 余る。このとき，a を 30 で割った余りを求めよ。

解 最初に

$15x\equiv 1 \pmod 2$, $10y\equiv 1 \pmod 3$, $6z\equiv 1 \pmod 5$

を満たす x, y, z を求める。ここに，$15x$ の 15 は mod3 と mod5 の数字 3 と 5 を掛けたものである。

求める x, y, z はただちに，

$$x=1,\ y=1,\ z=1$$

であることがわかる。このとき，問題の条件を満たす数 (の 1 つ) a は

$$a=1\times 1\times(3\times 5)+2\times 1\times(2\times 5)+3\times 1\times(2\times 3)$$
$$=1\times 15+2\times 10+3\times 6=53$$

である。実際，

$$a=1\times 15+2\times 10+3\times 6\equiv 1\times 15\equiv 1 \pmod 2,$$
$$a=1\times 15+2\times 10+3\times 6\equiv 2\times 10\equiv 2 \pmod 3,$$
$$a=1\times 15+2\times 10+3\times 6\equiv 3\times 6\equiv 3 \pmod 5$$

となる。

よって，求める余りは，53 を 30 で割ることにより，23 である。□

この 23 は 2 で割ると 1 余り，3 で割ると 2 余り，5 で割ると 3 余る数になっています。

上記の解答の流れを，下記のような表にすると一目瞭然になります。

	15	10	6	1×15	2×10	3×6
2 で割った余り	1	0	0	1	0	0
3 で割った余り	0	1	0	0	2	0
5 で割った余り	0	0	1	0	0	3

問題 2 は問題 1 より面白い問題になっています。

この問題の一般化を考えてみましょう。

l，m，n を互いに素な自然数とし，a，b，c を任意の整数とします。このとき，l で割ると a 余り，m で割ると b 余り，n で割ると c 余る数 A を lmn で割ったときの余り R を求める問題になります。

中国式剰余定理から

$$Z/lmnZ\cong(Z/lZ)\times(Z/mZ)\times(Z/nZ)$$

が成り立ちますので，求める余り R は 0 から $lmn-1$ の間にただ 1 つ存在します。後は余りの求め方になります。

最初に，

$mnx\equiv1\,(\mathrm{mod}\,l)$，$nly\equiv1\,(\mathrm{mod}\,m)$，$lmz\equiv1\,(\mathrm{mod}\,n)$

を満たす x，y，z を求めます。それらの存在は「2 つの整数 a，b が互いに素ならば，任意の整数 c について $ax+by=c$ を満たす整数 x，y が存在する」というよく知られている事実から保証されます。

そこで，$x=s$，$y=t$，$z=u$ としましょう。

このとき，

$$A=a(mn)s+b(nl)t+c(ml)u$$

を作ると

$$A\equiv a\,(\mathrm{mod}\,l),\quad A\equiv b\,(\mathrm{mod}\,m),\quad A\equiv c\,(\mathrm{mod}\,n)$$

となります。この A を lmn で割った余り R が求める数になります。なお，

$$R\equiv a\,(\mathrm{mod}\,l),\quad R\equiv b\,(\mathrm{mod}\,m),\quad R\equiv c\,(\mathrm{mod}\,n)$$

であることは，A を lmn で割ったときの商を B とすると

$$R=A-lmnB\quad(0\leqq R\leqq lmn-1)$$

であることから明らかです。

問題 1，2 とも問題文の内容が分かりやすい上に身近に感じられる問題なので生徒達の興味を引くことができるのではないでしょうか。

最後に問を 1 つ与えて本稿を閉じることにします。

問　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。

答　52

《参考文献》

〔1〕　藤田亮介　私信 (Private communication)

〔2〕　大島利雄他　数学A　数研出版

〔3〕　雪江明彦　代数学 1　群論入門　日本評論社

〔4〕　石井俊全　ガロア理論の頂を踏む　ベル出版

〔5〕　飯高　茂　群論，これはおもしろい　トランプで学ぶ群　共立出版

（元茨城県立藤代高等学校教諭）