中国式剰余の定理の構造と，問題解法の研究

青田（あおた）　義一（よしかず）

概要

（まずは概要でこの記事の流れを述べています．また，概要に出てくる問や定理の番号は本文中のものに対応しています．（編集部　注））

問3.2　3で割ると2余り，5で割ると3余り，7で割ると4余る整数xを求めよ．

という問のためには，xは幾通りもあるが，$3\times5\times7=105$ で割った余りは1通りに決まるという昔から知られた内容を確認した方がよい．

整数aとbを整数mで割った余りが等しいとき，$a\equiv b \pmod m$と表記し，aとbはmを法として合同というなら，xを3で割ると2余るという条件は，$x\equiv2 \pmod 3$という表記になる．

上記の余りに関する定理は，

定理3.3　**（中国式剰余の定理）**

$n_1, n_2, \cdots\cdots, n_k$を，どの2つをとっても互いに素な整数とするとき，連立方程式

$$\begin{cases} x\equiv r_1 \pmod{n_1} \\ x\equiv r_2 \pmod{n_2} \\ \quad\cdots\cdots \\ x\equiv r_k \pmod{n_k} \end{cases}$$

は，積 $N=n_1n_2\cdots\cdots n_k$ を法としてただ1つの解をもつ．

この定理の構造を調べていたところ，定理の構造・定理の証明・具体的問題への適用が密接に関連する方法を見出すことができた．その方法は，大学生に代数学の初歩の教材を与えるよい方法とも思われる．

端的に言えば，第3節の図5である．その図は次の問に答えるすべを教えてくれる．

問3.1　次の連立方程式を解け．

$x\equiv3 \pmod7$，$x\equiv2 \pmod5$

1　ユークリッドの互除法

次の定理は，高校内容である．（一意性までは言わないだろうが）

定理1.1　**（商と余りの一意性）**

整数mと$n(\neq0)$に対し，$m=nq+r$ $(0\leqq r<|n|)$をみたす整数q，rが存在して，しかも1通りに決まる．（一意的に決まる）

このとき，mをnで割ったときの商はq，余りはrという．さて，整数m，nの最大公約数dを$d=(m, n)$と表そう．

定理1.2　整数mを整数nで割ったときの余りをrとすると，$(m, n)=(r, n)$となる．

この定理がユークリッドの互除法の基本である．高校でユークリッドの互除法を以前教えたとき，直感的に理解させようと，次のような工夫を試みたことがある．

例1.1　$\frac{30}{12}$の分母と分子を$(30, 12)=6$で割って既約分数$\frac{5}{2}$とする．ところで，$\frac{30}{12}=\frac{12\times2+6}{12}$ $=2+\frac{6}{12}$とし，$\frac{6}{12}$の分母分子を$(6, 12)$で割って$2+\frac{1}{2}$とする場合と，$\frac{30}{12}=\frac{5}{2}=2+\frac{1}{2}$とする場合を比べてみよう．

$$\begin{array}{ccc} \frac{30}{12} & \longrightarrow & 2+\frac{6}{12} \\ \Big\downarrow \div(30,\ 12) & & \Big\downarrow \div(6,\ 12) \\ \frac{5}{2} & \longrightarrow & 2+\frac{1}{2} \end{array}$$

結果は同じはずだから，$(30, 12)=(6, 12)$である．■

m を n で割ったときの商 q，余り r を $\frac{m}{n}=q+\frac{r}{n}$ の形で扱おうという訳である．ところで，定理 1.2 の証明は次の補題を証明することで得られる．公約数の集合 2 つが一致すれば，それらの最大値（最大公約数）は同じになるから．

補題 1.3 整数 m を整数 n で割ったときの余りを r とするとき，m，n の公約数全体の集合 A と，r，n の公約数全体の集合 B とは，一致して $A=B$ である．

証明 m を n で割ったときの商を整数 q とすると，$m=nq+r$ である．

まず，$A\supset B$ を示す．B の任意の元 x に対し，$\frac{r}{x}$，$\frac{n}{x}$ はともに整数だから，$\frac{m}{x}=\frac{nq+r}{x}=\frac{n}{x}q+\frac{r}{x}$ は整数である．$\frac{m}{x}$，$\frac{n}{x}$ がともに整数であることが示されたから，$x\in A$ である． $\therefore\ A\supset B$

次に，$A\subset B$ を示す．$x\in A$ とすると，$\frac{m}{x}$，$\frac{n}{x}$ はともに整数だから，$\frac{r}{x}=\frac{m-nq}{x}=\frac{m}{x}-\frac{n}{x}q$ は整数．よって，$x\in B$ $\therefore\ A\subset B$

$A\subset B$ かつ $A\supset B$ より，$A=B$ ■

さて，ユークリッドの互除法．

系 1.4（ユークリッドの互除法）

正の 2 整数 m，n に対し，$r_0=n$ とおき，

m を r_0 で割った余りを r_1 とし，以下

r_0 を r_1 で割った余りを r_2，

r_1 を r_2 で割った余りを r_3，

r_2 を r_3 で割った余りを r_4，

……

とすると，この余りを互いに割る過程のどこかで $r_k=0$ となり，m，n の最大公約数について $(m,\ n)=r_{k-1}$ が成り立つ．

証明 $0\leqq r_{i+1}<r_i$ だから，$r_k=0$ となる整数 k がなければならない．

このとき，定理 1.2 より，

$(m,\ n)=(n,\ r_1)=(r_1,\ r_2)=(r_2,\ r_3)=\cdots\cdots$

$=(r_{k-2},\ r_{k-1})=r_{k-1}$ ■

この系の内容を直感的に示す方法を工夫すると，

例 1.2 $(900,\ 168)$ を求める．$900\div168$ の商 5，余り 60 より，$\frac{900}{168}=5+\frac{60}{168}$

例 1.1 より，$(900,\ 168)=(60,\ 168)$

$\frac{60}{168}$ の逆数をとって，$\frac{168}{60}=2+\frac{48}{60}$

さらに，同様 $\frac{60}{48}=1+\frac{12}{48}$ $\frac{48}{12}=4$

$\therefore\ (900,\ 168)=(60,\ 168)=(48,\ 60)=(12,\ 48)=12$

実際の計算は

①	5	900	168	2	②
		840	120		
③	1	60	48	4	④
		48	48		
		12	0		

よって，$(900,\ 168)=12$

ただし，①～④の数字は計算の順序を示し，それぞれ ① $900\div168$ ② $168\div60$ ③ $60\div48$ ④ $48\div12$ を表す．

2 代数学の基本定理と群構造

前節のユークリッドの互除法の考え方を突き詰めると，代数学の基本定理の 1 つを含む次の定理群が得られる．まず，記号の確認をして，次に定理群を証明無しに述べる．

$a|b$ とは，a が b の約数のこと．

$d=(m,\ n)$ とは，d が m，n の最大公約数であること．

$a\equiv b\ (\mathrm{mod}\,m)$ とは，a，b の各々を m で割った余りが等しいこと．即ち，$a-b$ が m の倍数であること．

定理 2.1（代数学の基本定理）

整数 m，n が互いに素，即ち $(m,\ n)=1$ ならば，$mx+ny=1$ をみたす整数 x，y が存在する．逆に，整数 m，n に対し，$mx+ny=1$ をみたす整数 x，y が存在するならば，$(m,\ n)=1$ である．

系 2.2 最大公約数が $(m,\ n)=d$ である整数 m，n に対し，$mx+ny=d$ をみたす整数 x，y が存在する．

定理 2.3 整数 m，n，r に対し $(m,\ n)=1$ のとき，方程式 $mx\equiv r\ (\mathrm{mod}\,n)$ は n を法としてただ 1 つの整数解をもつ．

系 2.4　整数 m, n, r に対し,
方程式 $mx\equiv r \pmod n$ は, r が $(m, n)=d$ の倍数であるときのみ整数解をもち, その解の個数は n を法として d 個である.

定理 2.5　$(m, n)=1$ ならば, $|n|$ 個の数 $0m$, m, $2m$, ……, $(|n|-1)m$ を n で割ったときの余りの集合は, $\{0, 1, 2, \cdots\cdots, |n|-1\}$ に等しい.

また, よく知られているように, 1 の n 乗根の全体 G は群をなし, $\zeta=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$ をとれば, $G=\{\zeta^n=1, \zeta, \zeta^2, \cdots\cdots, \zeta^{n-1}\}$ である. このように特定の元の累乗から作られる群を巡回群といい, 特定の元を巡回群の生成元という. 一般に, a を生成元とする巡回群を $\langle a\rangle$ で表す.

系 2.6　整数 n に対し, 複素数 $\zeta=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$ を生成元とする巡回群を $\langle\zeta\rangle=G$ とすれば, n と互いに素な整数 m に対し, ζ^m はまた G を生成する. 逆に, $\langle\zeta\rangle=\langle\omega\rangle$ となる ω は, $\omega=\zeta^m$ (m は n と互いに素) と表される場合に限る.

前節の例 1.1, 1.2 の方法で, 定理 2.1・系 2.2 を説明すると,

例 2.1　$m=900$, $n=168$ のとき, (m, n) を求める.
$\frac{900}{168}=5+\frac{60}{168}$, $\frac{168}{60}=2+\frac{48}{60}$, $\frac{60}{48}=1+\frac{12}{48}$, $\frac{48}{12}=4$ で, $(900, 168)=(60, 168)=(48, 60)=(12, 48)=12$ である. この変形を文字 m, n で表してみると,

$\frac{60}{168}=\frac{m}{n}-5=\frac{m-5n}{n}$ (つまり $60=m-5n$)

$\frac{48}{60}=\frac{n}{m-5n}-2=\frac{-2m+11n}{m-5n}$ $(48=-2m+11n)$

$\frac{12}{48}=\frac{m-5n}{-2m+11n}-1=\frac{3m-16n}{-2m+11n}$ $(12=3m-16n)$

となるから, $(m, n)=3m-16n$ と表される.

定理 2.1 を使えば以後の定理・系は証明されるが, 群論の本では, 定理 2.5・系 2.6 の一般化した定理を示し, 定理群はその定理の系とする場合もある. 言い換えれば, これらの定理・系の多くは定理 2.1 と同値であるということになる.

この小論では, ユークリッドの互除法の考え方と基本定理の結び付きも明確にするために, また, 余りに関する群の構造に着目するためにも, 最初に定理 2.3 を証明することとする. (証明は第 4 節に掲げる)

証明の前に, 余りに関する群の構造を, 定理・系に関する具体例から見ていこう.

では, 系 2.6 の例から. $\zeta=\cos\frac{\pi}{4}+i\sin\frac{\pi}{4}$ とおくと, $\zeta^8=1$ だから, 1 の 8 乗根の全体は $\{1, \zeta, \zeta^2, \cdots\cdots, \zeta^6, \zeta^7\}$ で巡回群をなす. 単位元は 1 で, ζ^k の逆元は ζ^{8-k} である.

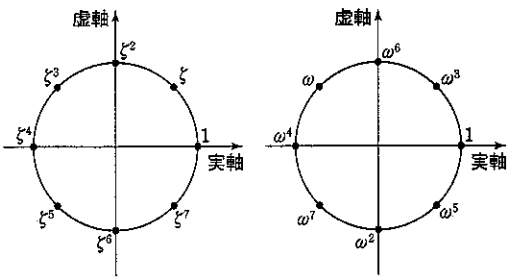


図 1：1 の 8 乗根

ド・モアブルの定理 $(\cos\theta+i\sin\theta)^n=\cos n\theta+i\sin n\theta$ に留意して, 複素平面上で図示すると, 図 1 の左図になるが, 右図は, $\omega=\zeta^3$ も同じ群を生成することを示す. $\left(\omega^k=\cos\frac{3k\pi}{4}+i\sin\frac{3k\pi}{4}\right)$

$\omega=\zeta^5$ や $\omega=\zeta^7$ の場合も, $\langle\zeta\rangle=\langle\omega\rangle$ である.

また, $\zeta^{8h+r}=(\zeta^8)^h\zeta^r=\zeta^r$, 即ち, $a\equiv b \pmod 8$ のとき, $\zeta^a=\zeta^b$ となる. 逆に, $\zeta^a=\zeta^b$ となる条件は $a\equiv b \pmod 8$ である.

上の例は, 余りだけに着目して演算を行う必要性を示している.

そこで, 整数全体の集合 $\mathbb{Z}$ を整数 n で割った余りで類別して, 集合 $A_r=\{nk+r \mid k\in\mathbb{Z}\}$ とする. n で割った余りの等しい数を同一視して, 集合 A_0, A_1, A_2, ……, A_{n-1} を n 個の数のように考える.

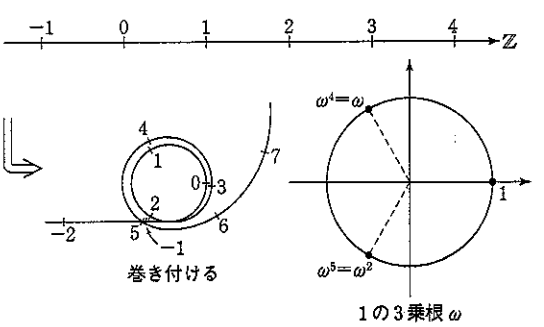


図 2：3 で割った余りで類別する

整数 a と (n を法として) 合同な整数全体 A_r を「a の代表する剰余類」と言い, $(a \mod n)$ または

単に a で表そう．すると，$a\equiv r \pmod n$ のときには $(a \mod n)=(r \mod n)$ あるいは単に $a=r$ である．

合同に関しては次の規則があり，集合の同値関係を表している．これらの規則はほとんど自明なので，証明は省略する．

法則 2.7

(1) $a\equiv a \pmod n$ [反射律]

(2) $a\equiv b \pmod n \Longrightarrow b\equiv a \pmod n$ [対称律]

(3) $a\equiv b \pmod n$, $b\equiv c \pmod n$
$\Longrightarrow a\equiv c \pmod n$ [推移律]

$\mathbb{Z}$ の n を法とする剰余類の集合を $\mathbb{Z}/n$ と表し $\mathbb{Z}/n=\{A_0, A_1, A_2, \cdots\cdots, A_{n-1}\}$ に 加減乗の演算 を定義する．つまり，

$(a \mod n)\pm(b \mod n)=(a\pm b \mod n)$

$(a \mod n)\times(b \mod n)=(a\times b \mod n)$

である．この定義は，剰余類の代表元の取り方によらないことを示して初めて，演算を定義することになるが，それは次の演算法則が成り立つからである．

法則 2.8

(1) $a\equiv a' \pmod n$, $b\equiv b' \pmod n$ ならば，
$(a\pm b)\equiv(a'\pm b') \pmod n$
特に，$a\equiv a' \pmod n$ ならば，
$(a\pm b)\equiv(a'\pm b) \pmod n$

(2) $a\equiv a' \pmod n$, $b\equiv b' \pmod n$ ならば，
$(a\times b)\equiv(a'\times b') \pmod n$
特に，$a\equiv a' \pmod n$ ならば，
$(a\times b)\equiv(a'\times b) \pmod n$

証明 (2) のみ証明する．(1) は同様に証明すればよいから．

a, b を n で割ったときの余りをそれぞれ r_1, r_2 とし，$r_1\times r_2$ を n で割ったときの余りを r_3 とすると，$a=np+r_1$, $a'=np'+r_1$, $b=nq+r_2$, $b'=nq'+r_2$, $r_1r_2=nQ+r_3$ となる整数 p, p', q, q', Q が存在する．

さて，$ab=(np+r_1)(nq+r_2)$
$=n(npq+pr_2+qr_1)+r_1r_2$
$=n(npq+pr_2+qr_1+Q)+r_3$ であり，
$a'b'=(np'+r_1)(nq'+r_2)$
$=n(np'q'+p'r_2+q'r_1)+r_1r_2$
$=n(np'q'+p'r_2+q'r_1+Q)+r_3$

余りの一意性により，ab, $a'b'$ を n で割ったときの余りはともに r_3 であり，$ab\equiv a'b' \pmod n$ が証明された． ■

ついでに，次の演算法則も述べておく．証明は上記の方法と同様にすればよいが，いま証明したばかりの演算法則を使う形へおき換えて証明する．

法則 2.9

(3) $a\equiv b \pmod n \iff ma\equiv mb \pmod{mn}$

証明 [$\Longrightarrow$] 法則 2.8 の(1)によれば，
$a\equiv b \pmod n \iff a-b\equiv 0 \pmod n$
よって，$a-b=nq$ をみたす整数 q が存在し，
$m(a-b)=(mn)q$ となるから，
$ma-mb\equiv 0 \pmod{mn} \iff ma\equiv mb \pmod{mn}$
[$\Longleftarrow$] $ma\equiv mb \pmod{mn} \iff ma-mb\equiv 0 \pmod{mn}$
よって，$m(a-b)=(mn)q$ をみたす整数 q が存在し，$a-b=nq$ となるから，
$a-b\equiv 0 \pmod n \iff a\equiv b \pmod n$ ■

注意：$a\equiv b \pmod n \Longrightarrow ma\equiv mb \pmod n$
は成り立つが，
$ma\equiv mb \pmod n \Longrightarrow a\equiv b \pmod n$
は成り立たない．(反例 $m=6$, $n=3$, $a=1$, $b=2$)

まだ証明していないが，定理 2.3 の拡張として，次の演算法則を挙げておく．理由は，ma を n で割ったときの余りを r とすると，a も b も
$mx\equiv r \pmod n$ の解になるが，$(m, n)=1$ により解の一意性があるから．

法則 2.10

(4) $(m, n)=1$, $ma\equiv mb \pmod n$ ならば，
$a\equiv b \pmod n$

以上，$\mathbb{Z}/n$ に加減乗の演算が定義されたが，演算 $+$ に関して $\mathbb{Z}/n$ は群となる．(加群という) 単位元は $(0 \mod n)$，$(a \mod n)$ の逆元は $(-a \mod n)=(-a+n \mod n)$ である．

定理 2.5 は，$\mathbb{Z}/n$ は n と互いに素な m の巡回群であることを示し，1 の n 乗根の全体のなす群 G と $\mathbb{Z}/n$ とは，群として同型 $G\cong\mathbb{Z}/n$ となることも言っている．(図 2 は，同型をイメージ化した図となっている)

ところが，$\mathbb{Z}/n$ の図を，図 2 のように数直線を円周上に巻き付けて表すことが難しい場合も多い．例えば，$(a \mod n)$ と $(b \mod m)$ とを組み合わせて

考える場合，組$((a \mod n), (b \mod m))$は紙の上には図示できない．そこで，次のようにする．

$\mathbb{Z}/5$で例示してみよう．剰余類$(a \mod 5)$を単にaと表記する方法で示す．

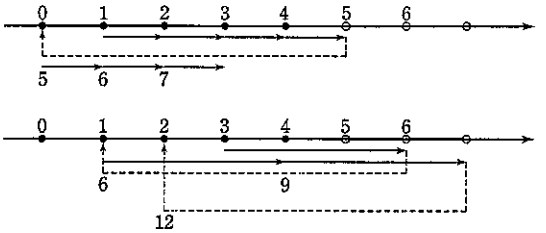


図3：$\mathbb{Z}/5$の元の図示

図3において，順に1を加えてゆくと数直線上では+1ずつ移動し，1→2→3→4→5となるが，5=0だから5の位置へ来れば即0へ移す．即ち，

1→2→3→4→5=0→6=1→7=2→……

順に3ずつ加える場合をやってみよう．

3→6=1→9=4→12=2→15=0 のように5以上になればすぐに−5移動する．

最後に，図1，2，3に関連して，ユークリッドの互除法の例を数直線上に図示しておこう．

$\frac{48}{18}=2+\frac{12}{18}$，$\frac{18}{12}=1+\frac{6}{12}$ より，

(48, 18)=(18, 12)=6 であるが，48，18，12はすべて最大公約数6で割れることを，図4のように示そう．

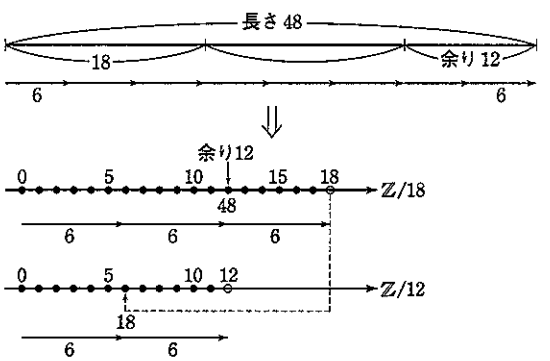


図4：互除法と剰余類

いよいよ，この節の定理群の証明にかかることになるが，証明は第4節にまとめる．

この節の定理群の証明無くして中国式剰余の定理を論じることはできない．しかし，中国式剰余の定理に含まれる群の構造に焦点を当てるためには，証明を後回しにして次節に進んだ方がよい．

3　中国式剰余の定理の群構造

概要で述べた中国式剰余の定理を，簡単な形の具体例で調べてみよう．

例3.1　連立合同方程式

$$\begin{cases} x\equiv 3 \pmod 7 \\ x\equiv 2 \pmod 5 \end{cases}$$

の解を調べる．一般にxを7，5で割った余りをそれぞれs，tとし，写像$f: x\to(s, t)$を考える．(s, t)はst座標平面上に点として図示するとよい．xが1増えると(s, t)は$(s+1, t+1)$となるから，$x=0, 1, 2, 3, \cdots\cdots$に対する点$(s, t)$を書き入れていくと，図5のようになる．

ただし，点(s, t)が直線$t=5$の上に来ればすぐに点$(s, 0)$へ移し，点(s, t)が直線$s=7$の上に来ればすぐに点$(0, t)$へ移す．図からは，写像fによって，集合$\{0, 1, 2, \cdots\cdots, 33, 34\}$と格子点の集合$\{(s, t)\mid 0\leqq s<7,\ 0\leqq t<5,\ s\in\mathbb{Z},\ t\in\mathbb{Z}\}$が1対1に対応していることが見て取れる．なぜか？

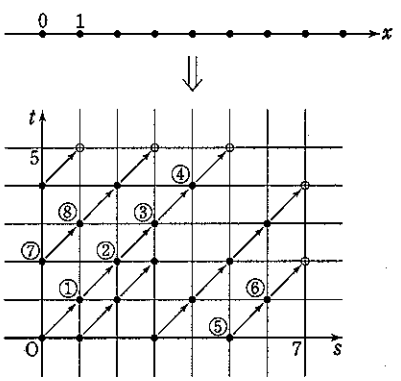


図5：$x\equiv 3 \pmod 7$，$x\equiv 2 \pmod 5$

xが0から5ずつ増えるときの点(s, t)に着目しよう．$f(0)=(0, 0)$，$f(5)=(5, 0)$，$f(10)=(3, 0)$，$f(15)=(1, 0)$，…… であるが，$10\equiv 3 \pmod 7$，$15\equiv 1 \pmod 7$，$20\equiv 6 \pmod 7$，……

だから，s軸上で図3と同じように$\mathbb{Z}/7$の元を図示したものとみなせる．即ち，$\mathbb{Z}/7$の元として，

0，5，10=3，15=1，20=6，25=4，30=2，35=0

である．定理2.5により，$\{f(5k)\mid 0\leqq k<7,\ k\in\mathbb{Z}\}=\{(s, 0)\mid 0\leqq s<7,\ s\in\mathbb{Z}\}$だから，写像$f$によって，集合$\{0, 1, 2, \cdots\cdots, 33, 34\}$と格子点の集合$\{(s, t)\mid 0\leqq s<7,\ 0\leqq t<5,\ s\in\mathbb{Z},\ t\in\mathbb{Z}\}$とが1対1に対応しているのだ．

この図の群構造に着目すると，連立合同方程式 $x\equiv 3 \pmod 7$, $x\equiv 2 \pmod 5$ を解く方法を発見できる．実際に解いてみるので，式変形の意味を図5の上で考えて頂きたい．

法則2.8により，$x-2\equiv 1 \pmod 7$ …… ①，$x-2\equiv 0 \pmod 5$ …… ② ②より，$x-2=5y$ $(y\in\mathbb{Z})$ とおけるから，①より $5y\equiv 1 \pmod 7$ 定理2.3により，y は7を法として1通りに決まるが，その値は $y=1, 2, \cdots\cdots$ を代入して確かめていくと，$y\equiv 3 \pmod 7$ であることが分かる．したがって，法則2.9により，$5y\equiv 5\times 3 \pmod{5\times 7}$ である．$x-2\equiv 15 \pmod{35}$ $\therefore\ x\equiv 17 \pmod{35}$ ■

それでは，例3.1の方法をそのまま，中国式剰余の定理の証明に用いてみよう．(ただし，定理2.3を使う証明になるので，厳密には第4節をここで読み込まねばならないが……)

補題 3.1

m, n は互いに素な整数とするとき，連立方程式

$$\begin{cases} x\equiv p \pmod m \\ x\equiv q \pmod n \end{cases}$$

は，mn を法としてただ1つの解をもつ．ただし，p, q は整数である．

証明 法則2.8により，$x-p\equiv 0 \pmod m$ …… ①，$x-p\equiv q-p \pmod n$ …… ② ①より，$x-p=my$ $(y\in\mathbb{Z})$ とおけるから，②より $my\equiv q-p \pmod n$ 定理2.3により，$(m, n)=1$ だから y は n を法として1通りに決まる．その値を $y\equiv y_0 \pmod n$ としよう．すると，法則2.9により，$my\equiv my_0 \pmod{mn}$ と同値である．同値関係に着目すると，

$$\begin{aligned} &\begin{cases} x\equiv p \pmod m \\ x\equiv q \pmod n \end{cases} \\ \Longleftrightarrow\ &\begin{cases} x-p=my\ (y\in\mathbb{Z}) \\ my\equiv q-p \pmod n \end{cases} \\ \Longleftrightarrow\ &\begin{cases} x-p=my \\ y\equiv y_0 \pmod n \end{cases} \\ \Longleftrightarrow\ &\begin{cases} x-p=my \\ my\equiv my_0 \pmod{mn} \end{cases} \\ \Longleftrightarrow\ &x-p\equiv my_0 \pmod{mn} \\ \Longleftrightarrow\ &x\equiv p+my_0 \pmod{mn} \end{aligned}$$ ■

問3.2 3で割ると2余り，5で割ると3余り，7で割ると4余る整数 x を求めよ．

解 x の方程式は，$x\equiv 2 \pmod 3$ …… ①，$x\equiv 3 \pmod 5$ …… ②，$x\equiv 4 \pmod 7$ …… ③ である．

①，②より，$x-2\equiv 0 \pmod 3$, $x-2\equiv 1 \pmod 5$ だから，$x-2=3y$ とおき，$3y\equiv 1 \pmod 5$ をみたす y を調べると，$y\equiv 2 \pmod 5$ に限る．$y\equiv 2 \pmod 5$ $\Longleftrightarrow$ $3y\equiv 6 \pmod{15}$ $\Longleftrightarrow$ $x-2\equiv 6 \pmod{15}$ $\therefore\ x\equiv 8 \pmod{15}$ …… ④

③，④より，$x-4\equiv 0 \pmod 7$, $x-4\equiv 4 \pmod{15}$ だから，$x-4=7z$ とおき，$7z\equiv 4 \pmod{15}$ をみたす z を調べると，$(7, 15)=1$ だから $z\equiv 7 \pmod{15}$ に限る．$z\equiv 7 \pmod{15}$ $\Longleftrightarrow$ $7z\equiv 49 \pmod{105}$ $\Longleftrightarrow$ $x-4\equiv 49 \pmod{105}$ $\therefore\ x\equiv 53 \pmod{105}$

ゆえに，求める x は $x=105n+53$ (n は整数) である．

補題 3.2 整数 n_1, n_2, ……, n_i, n_{i+1} を，どの2つをとっても互いに素な整数とするとき，積 $n_1n_2\cdots\cdots n_i$ と n_{i+1} は互いに素である．

注：自然数の素因数分解の一意性定理を使えば，自明な補題であり，実際，補題4.3より素因数分解の一意性定理は証明できるのだが，ここでは直接補題4.3から導いた．

証明 $(n_1n_2\cdots\cdots n_i,\ n_{i+1})=d$ に対し，$n_{i+1}=dn_{i+1}'$ としよう．$d\mid n_1n_2\cdots\cdots n_i$ より，$dn_{i+1}'\mid n_1n_2\cdots\cdots n_in_{i+1}'$ 即ち，$n_{i+1}\mid n_1n_2\cdots\cdots n_in_{i+1}'$

$(n_{i+1},\ n_1)=1$ だから，補題4.3により，$n_{i+1}\mid n_2\cdots\cdots n_in_{i+1}'$ でなければならない．

$(n_{i+1},\ n_2)=1$ だから，補題4.3により，$n_{i+1}\mid n_3\cdots\cdots n_in_{i+1}'$ でなければならない．

このようにして，$n_{i+1}\mid n_4\cdots\cdots n_in_{i+1}'$ $\Longrightarrow$ …… $\Longrightarrow$ $n_{i+1}\mid n_in_{i+1}'$ $\Longrightarrow$ $n_{i+1}\mid n_{i+1}'$

$n_{i+1}\mid n_{i+1}'$ は，$n_{i+1}=n_{i+1}'$ 即ち $d=1$ を表している． ■

定理 3.3 (中国式剰余の定理)

n_1, n_2, ……, n_k を，どの2つをとっても互いに素な整数とするとき，連立方程式

$$\begin{cases} x\equiv r_1 \pmod{n_1} & \cdots\cdots (1) \\ x\equiv r_2 \pmod{n_2} & \cdots\cdots (2) \\ \cdots\cdots \\ x\equiv r_k \pmod{n_k} & \cdots\cdots (k) \end{cases}$$

は，積 $N=n_1n_2\cdots\cdots n_k$ を法としてただ1つの解をもつ．

証明　補題3.1により，式(1)(2)をみたす x は n_1n_2 を法としてただ1つの解 r_2' をもつ．即ち，

(1)(2) $\Longleftrightarrow$ $x\equiv r_2' \pmod{n_1n_2}$ …… (2)′

すると，補題3.2より，$(n_1n_2,\ n_3)=1$ だから，補題3.1により，式(2)′(3)をみたす x は $n_1n_2n_3$ を法としてただ1つの解 r_3' をもつ．即ち，

(2)′(3) $\Longleftrightarrow$ $x\equiv r_3' \pmod{n_1n_2n_3}$ …… (3)′

さらに，補題3.2より，$(n_1n_2n_3,\ n_4)=1$ だから，補題3.1により，式(3)′(4)をみたす x は $n_1n_2n_3n_4$ を法としてただ1つの解 r_4' をもつ．即ち，

(3)′(4) $\Longleftrightarrow$ $x\equiv r_4' \pmod{n_1n_2n_3n_4}$ …… (4)′

このようにして，補題3.2と補題3.1により，中国式剰余の定理は帰納的に証明される．　■

4　第2節の定理群の証明

最初は，第2節の定理・系・補題のうち法則2.7, 2.8, 2.9以外は使わずに，定理2.3を証明する．

注：この節の証明は私が新たに証明し直したものですが，図1, 2, 3, 4の図示方法が，定理の証明に反映されています．例えば，次の補題4.1, 4.2は図4のイメージをおき換えたものです．

補題4.1　**（ユークリッドの互除法との関連付け）**

整数 M, n に対し，$M\equiv r \pmod n$, $n\equiv r' \pmod r$ のとき，$Mx\equiv r' \pmod n$ をみたす整数 x が存在する．

証明　$M=np+r$, $n=rq+r'$ (p, q は整数) とすると，$x=n-q$ に対し $Mx\equiv r' \pmod n$ であることを示すことができる．$M(n-q)=(np+r)(n-q)$
$=pn^2+(r-pq)n-rq=pn^2+(r-pq)n-(n-r')$
$=n(pn+r-pq-1)+r'$ だから，
$M(n-q)\equiv r' \pmod n$　■

補題4.2　整数 r に関する次の2つの条件は同値である．

(1)　$mx\equiv r \pmod n$ をみたす整数 x が存在する．

(2)　$ny\equiv r \pmod m$ をみたす整数 y が存在する．

また，$m\nmid n$ でもなく，$n\nmid m$ でもないとする．このとき，x がいろいろな整数値をとるとき，mx を n で割ったときの余り r のとる値の中で，0以外の最小値 r_1 が定まる．x がいろいろな整数値をとるとき，nx を m で割ったときの余り r のとる値の中で，0以外の最小値 r_2 が定まる．さらに，$r_1=r_2$ が成り立つ．

証明　条件(1)のとき，$mx=nq+r$ をみたす整数 q が存在する．$n(-q)=m(-x)+r$ だから，条件(2)が成り立つ．逆に，条件(2)のとき，同様に条件(1)が成り立つ．

後半の証明．$m\times x\equiv r \pmod n$ をみたす r の中に $r>0$ をみたすものが確かに存在する．[$n\nmid m$ でない，即ち $m\equiv 0 \pmod n$ でないから，$x=1$ の場合を考えればよい．] よって，r_1 は定まる．同様に r_2 が定まる．

$|m|>|n|$ としても一般性を失わない．

$0<r_1<|n|$ である．条件(1)(2)が同値だから，
$ny_1\equiv r_1 \pmod m$ をみたす整数 y_1 が存在する．
$0<r_1<|n|<|m|$ だから，r_2 の最小性より

$$r_2\leqq r_1 \quad \cdots\cdots ①$$

よって，$0<r_2<|n|$．r_1 の場合と同様，$mx_2\equiv r_2 \pmod n$ をみたす整数 x_2 があるが，$0<r_2<|n|$ だから，r_1 の最小性より　$r_1\leqq r_2$ …… ②

①，②より　$r_1=r_2$　■

定理2.3　整数 m, n, r に対し $(m,\ n)=1$ のとき，方程式 $mx\equiv r \pmod n$ は n を法としてただ1つの整数解をもつ．

注意：定理は2つの部分からなる．前半部分は，$mx\equiv r \pmod n$ は解をもつ，ということ．後半部分は，n を法として一意的に決まる，ということである．

前半の証明　整数 x がいろいろな値をとるとき，$mx\equiv R \pmod n$ $[0<R<n]$ をみたす R のうちで最小値を r_0 とすると，補題4.2により，r_0 は，
$nx\equiv R \pmod m$ $[0<R<m]$ をみたす R の最小値でもある．…… ⓐ

まず，$mx\equiv 1 \pmod n$ の解の存在を示す．そのための目標は，$r_0\nmid m$ かつ $r_0\nmid n$ である．r_0 は m, n の公約数となるが，$(m,\ n)=1$ より1以外の公約数はないからである．

$r_0\nmid n$ を示す．$mx_0\equiv r_0 \pmod n$ …… ① をみたす整数 x_0 がある．さて，n を r_0 で割った余りを r_1 とすると，$n\equiv r_1 \pmod{r_0}$ …… ②　補題4.1と①，②より，$(mx_0)x\equiv r_1 \pmod n$　即ち
$m(x_0x)\equiv r_1 \pmod n$ をみたす整数 x が存在する．

しかし，r_0 の最小性より，$r_1=0$ でなければならない．ゆえに，$n\equiv 0 \pmod{r_0}$　即ち，$r_0\nmid n$

さらに，$r_0|m$ を示すが，ⓐが成り立っているから，$r_0|n$ を示した方法と全く同様に，$r_0|m$ が言える．

$r_0|m$ かつ $r_0|n$ より，r_0 は m，n の公約数 1 であるから，$mx\equiv 1 \pmod n$ の解の 1 つは $x=x_0$

さて，$mx_0\equiv 1 \pmod n$ と法則 2 8 より，
$mx_0r\equiv 1\times r \pmod n$ が成り立つから，
$mx\equiv r \pmod n$ の解の 1 つは $x=x_0r$ である． ■

いまの証明は，実はユークリッドの互除法を間接的に使った証明である．この節の最後に，ユークリッドの互除法を直接使う証明のあらましを述べる．

定理 2.3 の後半の証明のために，前半の内容を使って，補題 4 3 を準備する．ただし，この補題は，素因数分解の一意性を証明するときに使う重要な定理である．

補題 4.3 整数 m，n，q について，$(m, n)=1$ のとき，$n|mq$ ならば $n|q$ である．

証明 $n|mq$ より，$mq\equiv 0 \pmod n$ …… ①
また，$(m, n)=1$ より，$mx_0\equiv 1 \pmod n$ …… ②
をみたす整数 x_0 がある．(定理 2.3 の前半は証明済)
②の両辺を q 倍して (法則 2.8)，
$q\equiv mx_0q \pmod n$ …… ③ ところで，①の両辺を x_0 倍して $mqx_0\equiv 0 \pmod n$ …… ④
③，④より，$q\equiv 0 \pmod n$ 即ち，$n|q$ ■

定理 2.3 の後半の証明
$mx_1\equiv r \pmod n$ かつ $mx_2\equiv r \pmod n$ ならば，
$x_1\equiv x_2 \pmod n$ をいう．
$mx_1-mx_2=m(x_1-x_2)\equiv 0 \pmod n$ だから，
$n|m(x_1-x_2)$ $(m, n)=1$ だから，補題 4 3 により，
$n|(x_1-x_2)$ 即ち $(x_1-x_2)\equiv 0 \pmod n$
$\therefore\ x_1\equiv x_2 \pmod n$ ■

注：上記，定理 2.3 の後半の証明は，法則 2.10 を直接示したものに他ならない．

定理 2.1 の証明 定理 2.3 において，
$mx\equiv 1 \pmod n$ をみたす x を x_0 とすれば，
$mx_0=nq+1$ (q は整数) $\therefore\ mx_0+n(-q)=1$

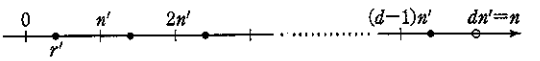
逆に，$mx+ny=1$ (x，y は整数) のとき，
$(m, n)=d$，$m=dm'$，$n=dn'$ とすると，
$d(m'x+n'y)=1$ よって，$d=1$ でなければならない． ■

系 2.2 の証明 $m=dm'$，$n=dn'$ とおくと，
$(m', n')=1$ だから，$m'x+n'y=1$ をみたす整数 x，y が存在する．$\therefore\ dm'x+dn'y=d$
よって，$mx+ny=d$ をみたす整数 x，y が存在する． ■

系 2.4 の証明 $(m, n)=d$，$m=dm'$，$n=dn'$ とする．

$mx\equiv r \pmod n$ が整数解 $x=x_0$ をもつとき，
$mx_0=nq+r$ (q は整数) 即ち，
$r=mx_0-nq=d(m'x_0-n'q)$ と表されるから，r は d の倍数でなければならない．

逆に，$d|r$ のとき，$r=dr'$ とおくと，法則 2.9 により，方程式 $mx\equiv r \pmod n$ 即ち
$dm'x\equiv dr' \pmod{dn'}$ は，$m'x\equiv r' \pmod{n'}$ と同値．
よって，定理 2.3 により，x は n' を法としてただ 1 つの解をもつ．$x=n'q+r'$ (q は整数)



よって，$mx\equiv r \pmod n$ は n を法として d 個の整数解をもつ．

定理 2.5 の証明 $|n|$ 個の数 $0m$，m，$2m$，……，$(|n|-1)m$ を n で割ったときの余りの集合を A，$B=\{0, 1, 2, \cdots\cdots, |n|-1\}$ とすると，$A\subset B$ である．Aの元の個数が $|n|$ であることを言えばよい．

定理 2.3 により，法則 2 10 は証明できる (第 2 節の法則 2.10 の記述直前の注を見て下さい)．したがって，$a\equiv b \pmod n$ でなければ，$am\equiv bm \pmod n$ でない．即ち，Aの元の個数は $|n|$

$A\subset B$ と併せて，$A=B$ が示された． ■

系 2.6 の証明については，定理 2.5 をそのまま利用すればよい．逆も，$(m, n)=d$ として，系 2.4 を使うと証明できる．この系は，この小論で剰余類の群の構造を示すためだけに用いているので，証明を割愛する．

最後に，定理 2 3 の前半部分を，ユークリッドの互除法を帰納的に直接使って証明する方法のあらましを述べる．

補題 4.4 (補題 4.1 の拡張) 整数 M，n，p に対し，
$M\equiv r \pmod n$，$np\equiv R \pmod r$ のとき，
$Mx\equiv R \pmod n$ をみたす整数 x が存在する．

証明の概略 $M=nq+r$，$np=rQ+R$ (q，Q は整数) とすると，$x=np-Q$ に対し $Mx\equiv R \pmod n$ であることを示すことができる． ■

定理 2.3 前半の証明の概略　$m=64$, $n=49$ の (m, n) を求めるユークリッドの互除法を mod で書き換えると,

$64\equiv 15 \pmod{49}$ …… ①
$49\equiv 4 \pmod{15}$ …… ②
$15\equiv 3 \pmod{4}$ …… ③
$4\equiv 1 \pmod{3}$ …… ④

だから, ③, ④に補題 4.4 を適用して,

$15x_1\equiv 1 \pmod{4}$ …… ③′

をみたす整数 x_1 が存在する. 次いで, ②, ③′に補題 4.4 を適用して,

$49x_2\equiv 1 \pmod{15}$ …… ②′

をみたす整数 x_2 が存在する. 最後に, ①, ②′に補題 4.4 を適用して,

$64X\equiv 1 \pmod{49}$

をみたす整数 X が存在する.

同様に, $(m, n)=1$ の場合の系 1.4 (ユークリッドの互除法) を書き換えて, 後ろから補題 4.4 を適用してゆけばよい. ■

5　最後に

実数係数の x の整式全体の集合を $\mathbb{R}[x]$, 有理数係数の x の整式全体の集合を $\mathbb{Q}[x]$, 複素数係数の x の整式全体の集合を $\mathbb{C}[x]$ としよう. $\mathbb{Z}$ に関するこの小論の内容は, $\mathbb{R}[x]$ や $\mathbb{Q}[x]$ における内容におき換えることができる.

$\mathbb{R}[x]$ や $\mathbb{Q}[x]$ や $\mathbb{C}[x]$ での理論化は, 省略するので各自確かめて欲しい.

最後の最後に, 2 つの事項を.

(I)　補題 3.1 の解が対称形になっていない不満に対して. 一般に, 定理 3.3 の解について, ガウスの考案したという方法を示しておきます.

$N=n_1n_2\cdots\cdots n_k$ に対し $N_i=\dfrac{N}{n_i}$ とすると,

$(n_i, N_i)=1$ より　$N_iy\equiv 1 \pmod{n_i}$ をみたす整数 $y=y_1$ がある.

$x\equiv N_1y_1r_1+N_2y_2r_2+\cdots\cdots+N_ky_kr_k$ が求める解であるという.

解かどうかを確かめると同時に, ガウスがどのように発見したのかに思いめぐらすのも面白い.

(II)　例 3.1 や問 3.2 の具体例で示した解法について, $(m, n)=1$ だが $|m|$, $|n|$ が大きな数の場合,

$my\equiv r \pmod{n}$ の解を求めるのに, $y=1$, 2, ……, $|n|$ を順に代入して探すことは実用的でない. どうすればよいか.

例えば, $m=728$, $n=495$, $my\equiv 50 \pmod{n}$ に対して

	1	728	495	2
		495	466	
	8	233	29	
		232		
		1		

	1	m	n	2
		n	$2m-2n$	
つまり	8	$m-n$	$-2m+3n$	
		$-16m+24n$		
		$17m-25n$		

$17m-25n=1$ となるから, $my\equiv 1 \pmod{n}$ の解は $y\equiv 17 \pmod{n}$

したがって, $m\times 17\times 50\equiv 1\times 50 \pmod{n}$

となって $my\equiv 50 \pmod{n}$ の解は

$y\equiv 17\times 50\equiv 355 \pmod{495}$ と解けるのだが,

mod の式だけ使って求めるうまい方法があれば, ご教示下さい.

《参　考　文　献》

[1] 草場公邦 著『ガロワと方程式』
(朝倉書店　すうがくぶっくす 7　1989 年)
[2] 浅野啓三・永尾汎 著『群論』
(岩波全書　1965 年)
[3] 志賀弘典 著『数学おもちゃ箱』
(日本評論社　1999 年)

(兵庫県立福崎高等学校)