中国剰余定理

藤田 博司

2013 年 12 月 17 日

1　倍数と約数

整数 a の **倍数** とは，ax $(x \in \mathbb{Z})$ の形の整数，いいかえれば

$$\ldots, -2a, -a, 0, a, 2a, 3a, \ldots$$

のことです．b が a の倍数であるとき，a は b を **割り切る** といいます．また，a は b の **約数** である，ともいいます．このことを $a \mid b$ と書きます：

$$a \mid b \iff \exists x \in \mathbb{Z}\,(b = ax).$$

整数 a の倍数全体の集合を $a\mathbb{Z}$ と書きます．
単数 1 はすべての整数の約数です．0 はすべての数の倍数です．整数 a は a 自身の倍数であり約数です．

■例　$15 = 5 \times 3$ なので，15 は 3 の倍数です．$105 = 35 \times 3$ なので，105 も 3 の倍数です．115 は 3 の倍数ではありません．$115 = 38 \times 3 + 1$ で，1 が余ります．

$$15 \in 3\mathbb{Z}, \quad 105 \in 3\mathbb{Z}, \quad 115 \notin 3\mathbb{Z}.$$

■練習　(1) 11 の倍数と倍数でないものの例について，このように説明する文章を書いてごらんなさい．
(2) 整数 120 の正の約数をすべて書き出しなさい．

2　最大公約数

ふたつの整数 a と b があったとき，$x \mid a$ かつ $x \mid b$ をみたす整数 x のことを a と b の **公約数** といいます．

■例　120 と 105 の正の公約数は 1,3,5,15 の 4 つあります．

■練習　120 と 108 の正の公約数をすべて書き出しなさい．

単数 1 はすべての整数の約数なので，どんな 2 つの整数についても正の公約数は必ず少なくともひとつは存在します．また，その個数は有限個です (整数 a の正の約数はすべて $|a|$ 以下だからです)．そこで，ふたつの整数 a と b の正の公約数のうちで最大のものが存在することになります．それを a と b の **最大公約数** といい，$\gcd(a, b)$ と書きます．“gcd” は greatest commond divisor の略です．

■例　120 と 105 の最大公約数は 15 です．

■練習　120 と 108 の最大公約数はいくつですか.

最大公約数についての次の補題は有用です.

補題 1　整数 a と b の最大公約数を d とするとき，$ax+by=d$ をみたす整数 x と y が存在する.

補題を証明する前に例をやりましょう.

■例　(1) 整数 120 と 105 の最大公約数 15 については簡単で，$120-105=15$ なので $x=1$，$y=-1$ です．(2) 整数 174 と 231 の最大公約数は，素因数分解で調べてみると 3 であることがわかります.

$$174\times 4-231\times 3=3$$

なので，この場合は $x=4$，$y=-3$ です．このような x と y を見つける方法は，次のセクションで説明します.

■補題 1 の証明　整数 a と b が与えられたとしよう．a と b の一方または両方ともがゼロなら補題は自明に成立するので，以下では a も b もゼロではないと仮定する.

(i) $ax+by$ $(x,y\in\mathbb{Z})$ の形の整数全体の集合を G としよう：

$$G=\{\,ax+by\,:\,x,y\in\mathbb{Z}\,\}.$$

集合 G は足し算と引き算のもとで閉じている．また $a=a\cdot 1+b\cdot 0$，$b=a\cdot 0+b\cdot 1$ なので $a,b\in G$ である.

(ii) たとえ $a<0$ であっても $-a>0$ かつ $-a\in G$ なので，G には正の整数が少なくとも 1 つは属している．だから，G の正の要素のうち最小のものが存在する．それを c とする．整数 x_0 と y_0 を

$$c=ax_0+by_0$$

となるようにとろう.

(iii) 集合 G は足し算と引き算のもとで閉じているので，c の倍数はみな G に属する．すなわち $c\mathbb{Z}\subset G$ である.

(iv) 次に $G\subset c\mathbb{Z}$ であることを示す．$g\in G$ を G の任意の要素として，これを c で割って

$$g=qc+r\quad(0\le r<c)$$

のように，商 q と余り r を得たとしよう．このとき,

$$r=g-qc\in G$$

であるから，c の最小性条件から $r=0$ である．すなわち，$g=qc$ で，g は c で割り切れる．したがって $g\in c\mathbb{Z}$ である．このことから $G\subset c\mathbb{Z}$ となることがわかる.

(v) これで $G=c\mathbb{Z}$ であることがわかった．ところが，$a\in G$，$b\in G$ であったから a も b も c の倍数，したがって c は a と b の公約数である.

(vi) ここで，a と b の最大公約数 d を考える．整数 a' と b' を，$a=a'd$，$b=b'd$ となるようにとろう．すると,

$$c=ax_0+by_0=a'dx_0+b'dy_0=d(a'x_0+b'y_0)$$

であるから，c も d の倍数である．いま c も d も正の数なので，このことから $d\le c$ である.

(vii) ところが (v) より c は a と b の公約数で，d は最大公約数であるから，$0<c\le d$ のはず．したがって $c=d$ である．こうして $d=c=ax_0+by_0$ と書けることがわかった．[**証明終**]

■練習　補題の証明の最初に「自明に成立する」と言われた $a = 0$ または $b = 0$ の場合を，詳しく述べてみてください．

3　互除法

コンピュータなどで最大公約数を高速に求める手順として知られているのが「ユークリッドのアルゴリズム」，またの名を**「互除法」**というものです．これは

2 つの正整数の大きい方を，小さい方で割って，
大きい方の数を，その剰余に置き換える．
割り切れた時点での除数が，最大公約数である

という計算手順のことです．この手順がうまくいくことの数学的な証明は，ここでは省略します．百聞は一見にしかず．実例を示しましょう．次の表では，「大きい方の数を，小さいほうで割った剰余に置き換え，割った数が大きいほうに成り上がる」という手順が上から下へ進行していきます．

■例　(1) 整数 174 と 231 の場合．

大	小	剰余	商
231	174	57	1
174	57	3	3
57	3	0	19

したがって最大公約数は 3 です．

(2) 整数 2096 と 1017 の場合，

大	小	剰余	商
2096	1017	62	2
1017	62	25	16
62	25	12	2
25	12	1	2
12	1	0	12

したがって最大公約数は 1 です．

目的が最大公約数を求めることだけであれば，ここで計算途中に得られた商を書き留めておく必要はありませんが，商の情報を使えば $ax + by = \gcd(a, b)$ をみたす整数 x と y を計算することができます．たとえば例 (1) の 174 と 231 の場合，

$$\begin{aligned} 3 &= 174 - 57 \times 3 \\ &= 174 - (231 - 174 \times 1) \times 3 \\ &= 174 \times 4 - 213 \times 3, \end{aligned}$$

したがって $x = 4$，$y = -3$ となります．

例 (2) の整数 2096 と 1017 の場合,

$$\begin{aligned} 1 &= 25 - 12 \times 2 \\ &= 25 \times 5 - 62 \times 2 \\ &= 1017 \times 5 - 62 \times 82 \\ &= 1017 \times 169 - 2096 \times 82 \end{aligned} \qquad \begin{aligned} &= 25 - (62 - 25 \times 2) \times 2 \\ &= (1017 - 62 \times 16) \times 5 - 62 \times 2 \\ &= 1017 \times 5 - (2096 - 1017 \times 2) \times 82 \end{aligned}$$

したがって $x = -82$, $y = 169$ となります.

■練習　$a = 14096$, $b = 14208$ というペアについて上の例にならって最大公約数 d と方程式 $d = ax + by$ の解 x, y を求めなさい. 他のいろいろな整数のペア a, b についても試してごらんなさい.

4　整数の合同関係

正の整数 m が与えられたとしましょう. 二つの整数 x と y の差 $x - y$ が m の倍数であるとき, x と y は m **を法として合同** であるといい,

$$x \equiv y \pmod{m}$$

と書きます. これはまた, x と y をそれぞれ m で割ったら余りが等しい, ということでもあります. このことから, x と y の関係としての $x \equiv y \pmod{m}$ が「同値関係」であることは, ほとんど明らかです:

◇1 $x \equiv x \pmod{m}$;
◇2 $x \equiv y \pmod{m}$ ならば $y \equiv x \pmod{m}$ でもある;
◇3 $x \equiv y \pmod{m}$ で $y \equiv z \pmod{m}$ ならば $x \equiv z \pmod{m}$ である.

■練習　◇1〜◇3 を証明しなさい.

整数 x のこの同値関係に関する同値類を m **を法とした** x **の合同類** といい, m を法とした合同類の全体 (商集合) を, $\mathbb{Z}/m\mathbb{Z}$ と書くのでした. すなわち $\mathbb{Z}/m\mathbb{Z}$ は $\overline{0}, \overline{1}, \ldots, \overline{m-1}$ という m 個の要素からなり, 各要素 $\overline{x}$ は m を法とする合同関係に関する x の同値類, すなわち集合

$$\overline{x} = \{\ldots,\ x - 2m,\ x - m,\ x,\ x + m,\ x + 2m,\ \ldots\}$$

です.

合同関係は整数の和や積と「整合」します. というのは

◇4 $x_1 \equiv x_2 \pmod{m}$ かつ $y_1 \equiv y_2 \pmod{m}$ ならば $x_1 + y_1 \equiv x_2 + y_2 \pmod{m}$ である;
◇5 $x_1 \equiv x_2 \pmod{m}$ かつ $y_1 \equiv y_2 \pmod{m}$ ならば $x_1 y_1 \equiv x_2 y_2 \pmod{m}$ である

という意味です.

このため, 二つの整数 x と y についての合同類 $\overline{x+y}$ と $\overline{xy}$ は x と y の合同類 $\overline{x}$ と $\overline{y}$ が決まればそれで決まってしまいます. 代数学でよくやる「演算が well-defined である」ということです.

■練習　◇4, ◇5 を証明しなさい.

5　互いに素

二つの整数 a と b について $\gcd(a,b)=1$ であるとき，a と b は **互いに素** であるといいます．補題 1 によればこれは $ax+by=1$ となる整数 x と y がとれることと同値です．

■練習　いや，補題 1 は「$\gcd(a,b)=1$ ならばそのような x と y がとれる」としか言っていません．なぜ逆が成立するのでしょうか．考えてごらんなさい．

❑ 補題 1 によれば，整数 a と b が互いに素であれば，どんな整数も a の倍数と b の倍数の和であらわすことができます．$ax+by=1$ なら整数 c を $c=a(cx)+b(cy)$ とあらわせばよいのです．

合同関係を用いて補題 1 を書き直せば，次の補題が得られます．

補題 2　二つの正整数 a と b が互いに素であるためには，合同式

$$by \equiv 1 \pmod{a}$$

をみたす整数 y の存在することが，必要かつ十分である．

[**証明**] (必要であること) a と b が互いに素であるなら，$ax+by=1$ であるから $by-1=-ax$ であって，$by-1$ が a の倍数であるから $by\equiv 1 \pmod{a}$ である．

(十分であること) $by\equiv 1 \pmod{a}$ とすれば，$by-1$ は a の倍数なのであるから $by-1=ax$ とすれば $ax+b(-y)=1$ であって，補題 1(の逆) により $\gcd(a,b)=1$ となる．[**証明終**]

補題 3　整数 a, b, c があって，a と b が互いに素，a と c も互いに素であるとき，a と bc も互いに素である．

[**証明**] 補題 2 により，$by\equiv 1 \pmod{a}$ をみたす整数 y と $cz\equiv 1 \pmod{a}$ をみたす整数 z が存在する．このとき合同関係の性質◇5 から

$$(bc)(yz)=(by)(cz)\equiv 1\cdot 1\equiv 1 \pmod{a}$$

であるから，ふたたび補題 2 によって，a と bc は互いに素である．[**証明終**]

❑ 補題 3 の逆も成立します．すなわち，a と bc が互いに素であるとき，a と b は互いに素，a と c も互いに素です．このことは，補題 1 によって $ax+(bc)y=1$ となる整数 x と y をとってみれば明らかです．

6　中国剰余定理

定理 4　(中国剰余定理) どの 2 つも互いに素な 2 以上の整数が r 個 $a_1, a_2, \ldots, a_r$ と与えられているとする．また，r 個の任意の整数 $x_1, x_2, \ldots, x_r$ が与えられたとする．このとき，整数 y を

$$\begin{aligned} y &\equiv x_1 \pmod{a_1} \\ y &\equiv x_2 \pmod{a_2} \\ &\vdots \\ y &\equiv x_r \pmod{a_r} \end{aligned}$$

となるようにとれる．

❑ この定理が「中国剰余定理」(Chinese Remainder Theorem) と呼ばれるのは，西暦 400 年ごろ成立したとされる中国の算術書『孫子算経』に，この定理の原型が見出だせるからだそうです．ときの中国は六朝時代で，中央の実権を東晋王朝が握っていた頃のことです．のちの唐王朝 (西暦 618 年〜900 年ごろ) においては官吏の教育の初級の教科書として『孫子算経』が採用されたといいます．作者の「孫子」が誰かは不詳です．(情報源は `http://www.osaka-kyoiku.ac.jp/~jochi/j8.htm` でした．)

■定理 4 の証明　(i) 与えられた r 個の整数 $a_1, a_2, \ldots, a_r$ のうち，i 番めを除く $r-1$ 個の積を b_i と書こう：

$$b_i = a_1 \cdots a_{i-1} \cdot a_{i+1} \cdots a_r.$$

このとき補題 3 から a_i と b_i は互いに素である．また，$i \neq j$ のとき $a_i \mid b_j$ である．

(ii) 補題 2 により，

$$b_i y_i \equiv 1 \pmod{a_i}$$

をみたす整数 y_i がとれる．$b_i y_i = e_i$ とおいてみよう．すると，$i, j \in \{1, 2, \ldots, r\}$ に対して

$$e_j \equiv \begin{cases} 1 & j = i \text{ のとき} \\ 0 & j \neq i \text{ のとき} \end{cases} \pmod{a_i}$$

が成立する．

(iii) あとは，与えられた整数 $x_1, x_2, \ldots, x_r$ に対して

$$y = x_1 e_1 + x_2 e_2 + \cdots + x_r e_r$$

とおけば，この y が定理のいう要件をみたす．[**証明終**]

■練習　ここに書いた定理 4 の証明は細かいチェックを省略しています．(i) のように b_i をとればそれが a_i と互いに素であること，また，y を (iii) のようにとればうまくいくことを，きちんと検証してください．

■練習　$r = 2$, $a_1 = 5$, $a_2 = 9$ として証明の (ii) にいう e_1 と e_2 をみつけてください．

■練習　$a_1, a_2, \ldots, a_r$ が互いに素でないときには，$x_1, x_2, \ldots, x_r$ の選び方によっては，定理の要件をみたす y がとれないことがあります．$r = 2$ の場合にそのような実例を挙げてください．

■練習　与えられた $a_1, a_2, \ldots, a_r$ と $x_1, x_2, \ldots, x_r$ に対して，定理 4 の要件をみたす整数 y は一意的には決まりません．y_0 を定理 4 の要件をみたす整数のひとつとするとき，他の整数 y が同じ要件をみたすためには，$y \equiv y_0 \pmod{a_1 a_2 \cdots a_r}$ となることが必要かつ十分です．このことを証明してください．

✎✎✎✎ 研究課題 ✎✎✎✎

結城浩『数学ガールの秘密ノート〜整数で遊ぼう』(SB クリエイティブ, 2013 年) の第 5 章の内容は，中国剰余定理で $r = 3$, $a_1 = 2$, $a_2 = 3$, $a_3 = 5$ とした場合に対応しています．作中の人物「僕」とユーリがこの章で掘り下げた内容が，中国剰余定理の主張およびその証明と，どのように対応するか，考察してごらんなさい．

☆☆ 謹　呈 ☆☆

結城浩さまに

新刊『数学ガールの秘密ノート 整数で遊ぼう』発売の記念として
謹んで献呈いたします.

2013 年 12 月 17 日
藤田 博司