上越数学教育研究, 第 13 号, 上越教育大学数学教室, 1998 年, pp.23-32.

ユークリッドの互除法の一般化について

岩崎　浩

1　はじめに

本稿ではユークリッドの互除法の一般化について述べる。ユークリッドの互除法が2つの数の最大公約数を扱い，その繰り返しによってn個の整数の最大公約数を扱うのに対して，本稿で述べるユークリッドの互除法の一般化は，原理的にみてn個の整数の最大公約数をそのまま扱うところに特徴がある。

このようなユークリッドの互除法の一般化を取り上げる意図は，主に次の二つである。一つは，この一般化が，ある文脈からみれば非常に自然であるにも関わらず，余り知られていないということである。もう一つは，この一般化が，数学的関係それ自体への興味やその関係と応用可能性との関連，一般化の方法など，数学の幾つかの性格を例証しているからである。しかも，その内容を理解するのに特別な予備知識をほとんど必要としない。したがって，小・中学校の教師を志望している学生や，現職の小・中学校の教師が，数学についての適切な理解を得るのに少しでも役立ちうるのではないかと思ったからである。そして，このような教材を豊富に用意することは，教員養成系学部の重要な仕事の一部であると考えるからである。平林(1994a)は次のように述べている[1)]。

> そうした大学の卒業生が小学校の教師になったとき，どのような問題が起こるでしょうか。おそらく日常の授業実践については，先輩の諸先生がいろいろな面で親切に指導してくださるでしょうから，授業技術の点では，外見的にも著しい進歩が見られるようになるでしょう。しかし，そうした技術面でまじめに努力される方ほど，おそらくどうにもならない一種の虚無感に陥られるかもしれないと思います。たとえば，子どもにこんなことを教えて何になるのか，子どもはこんなことをどうしても知らなくてはならないのか，といった問題については，教育技術は何も教えてくれないからです。

ここで述べられている問題は，同氏が述べるように，教育技術の問題ではない。むしろ，思想性の問題である。この問題を解決するのは容易ではない。しかし，同氏も述べるとおり，その第一歩は，数学及び私がメタ知識と呼びたいところの，数学と人間性との関係の適切な理解に，できる限り具体的に，アプローチすることである。

平林(1994a)は，このアプローチとして教師自らが「数学する」[1]ことを挙げており，このような教師自らが数学する体験，「数学的体験」のための幾つかの教材を提供している。同氏はまた，「理学部の数学は歯のたたないステーキであり，教育学部の数学は肉の入らないスープである。」というある外国の雑誌からの一文を引用し，これまでの教員養成系学部では，世界的にみても，上の問題にアプローチするのに適した教材が積極的に提供されてこなかったと述べ，このような教材の開発の必要性を示唆している。

[1]これは，上越数学教育研究会やΣ会で，子どもたちに数学を指導する上での最も基本的な方法として重視されてきた考え方でもある[2)]。

本稿の試みも，教師志望の学生や現職の先生方にとって，数学及びそれと人間性との関連について反省したり，理解を深めるのに少しでも貢献しうるような教材を提供しようという一つの努力である。

2　ユークリッドの互除法の幾つかの意味

ユークリッドの互除法は，ユークリッド原論第7巻命題2にあるように[3]，最大公約数を求める一つのアルゴリズムとして最もよく知られている。一方，忘れてはならないのは，ユークリッドの互除法の歴史的意味であり，それは，無理数性を認識する道具としての意味である。無理数性は，正五角形の一辺とその対角線との間に見いだされたともいわれている。この無理数性の認識を支えているのがユークリッドの互除法である。2量の間に通約量（共通のものさし）が存在する場合には，ユークリッドの互除法は有限回で終了する。正五角形の一辺とその対角線の場合には，ユークリッドの互除法が果てしなく続くことがわかる[4][5]。無理数は，日常的に有用なものとして生起しない数であり，むしろ，理論的に異常なものとして生起する。その異常さは，論理によってはじめて認識しうるものである。学校数学では取り上げられないが，無理数は，この意味でも陶冶価値を有し[6]，ユークリッドの互除法は，この無理数の存在を最も具体的に認識するための一つの思考の道具である。ユークリッドの互除法がこのような道具たりうるのは，次節でも述べるが，そのアルゴリズム自体に素因数分解など，通約量の存在を仮定していないからである。

文部省の指導書によれば，最大公約数は，小学校第5学年の内容の中の「数と計算」において，特に，整数についての理解を深めるものとして位置づけられている。一方，中学校ではこの用語は出てこない[2]。

[2]中学校においては，最大公約数は取り扱われておらず，関連する内容としては，第3学年の学習内容である「多項式の因数分解」の中に自然数の素因数分解が位置づけられている。そして，「多項式の因数分解」の意味を理解するためのモデルとして，自然数の素因数分解が位置づけられている程度である。これを受けて，教科書でも，最大公約数に関する記述はなく，素数や素数の求め方などを取り上げる程度にとどめている。これらは，多項式の因数分解を自然数の因数分解をモデルとして理解するのに必要最小限の内容である[7][8]。

算数での最大公約数の取り扱いをみると『最大公約数及び最小公倍数を形式的に求めることに偏ることなく，具体的な場面に即して取り扱う程度とするよう配慮する必要がある。』[9]となっている。これを受けて，教科書[10]でも，例えば，$18cm \times 12cm$ の用紙に同じ大きさの正方形の紙をすき間なくならべるという場面を設定し，うめることができる一番大きい正方形の一辺の長さを求める問題が取り上げられている。そして，最大公約数を求める方法としては，18と12のそれぞれの約数を全て書き出し，公約数を○で囲み，その中で最大のものを選ぶという方法である。

このように，最大公約数を日常生活との関連で考えている限り，ユークリッドの互除法をあえて用いる必要性は出てこないように思われる。実際，ユークリッドの互除法の実用的意味が生じてくるのは，むしろ，より大きな数の最大公約数を求める必要がある場合や，それをコンピュータで機械的に求める必要が生じた場合に限られてくる。このことが最大公約数を取り上げているにも関わらず，歴史的及び実用的意味をもったユークリッドの互除法が小学校で積極的に取り扱われない一つの理由になっているように思われる。

しかし，小学校算数はそれ自身完結したものではなく，中学校数学の準備とみなされる現在の状況においては，小学校段階においても，日常生活との関連，すなわち，数や図形を生活に役立つ問題解決の道具としてだけでなく，それ以上に，それ自身興味ある対象として考えていけるように指導することが必要になってきている。

例えば，中学校数学の一つの特徴である「論証」には，ファン・ヒーレの学習水準の理論が典型的に例証しているように，数や図形を問題解決の道具としてだけではなく，それ自身興味ある対象として考えることが要求される。

本稿で取り上げるユークリッドの互除法の一般化も，問題解決の道具としてよりも，むしろ，ユークリッドの互除法の背景にある数の関係そのものへの関心に由来している。実用的な観点だけでなく，最大公約数やそれを求めるプロセスそのものへ目を向けようとしたとき，ユークリッドの互除法は，それ自身として興味ある関係を含んでいるように思われる。この関係は本学数学コースのある学部生によって見いだされた関係であるが，私自身にとっても興味深い一つの発見であった。

3　ユークリッドの互除法の一般化

3.1 予備的考察

ユークリッドの互除法は，最大公約数を求めるきわめて合理的な方法である。このことは次の最大公約数の求め方と比較するとわかりやすい。

2	42	30
3	21	15
[6]	7	5

図 1: 42 と 30 の最大公約数の求め方 (1)

この求め方は，42 と 30 の公約数を適当に見当をつけていき，それらをかけるという方法である。この方法は一見便利だが，目安で公約数となる数の見当をつけなければならないので，例えば，3569 と 4399 のような 2 数の最大公約数をこの方法で求めるのは難しいであろう。なぜなら，これら 2 数の素因数分解は，それぞれ，83×43，83×53 で表され，目安で見当をつけるには大きい素数の積になっているからである。

ユークリッドの互除法の特徴は，与えられた 2 数に対して，このような素因数分解を前提としない（しなくてよい）ところにある。ユークリッドの互除法が，前節でも述べたように，2 つの量の間に通約量が存在するかどうかを確認する手段となりうるのは，正に，この特徴によるものといえるであろう。

それでは，ユークリッドの互除法とはどのような方法なのか。42 と 30 の最大公約数をユークリッドの互除法で求めながら，具体的に述べることにしよう。

$$42 = 30 \times 1 + 12 \quad \text{(i)}$$
$$30 = 12 \times 2 + 6 \quad \text{(ii)}$$
$$12 = \boxed{6} \times 2 + 0 \quad \text{(iii)}$$

図 2: 42 と 30 の最大公約数の求め方 (2)

図 2 は，42 と 30 の最大公約数をユークリッドの互除法で求めているところを表している。除数と余りをそれぞれ被除数と除数に置き換えて，余りが 0 になるまで繰り返している。別の見方をすれば，余りで除数が割り切れるかどうかを常にチェックしているともみれる。そして，余りで除数がちょうど割り切れたとき，その余り (当該の式では除数になっている) の数が最大公約数である。

今の場合 6 が最大公約数であることがわかる。まず，6 が 42 と 30 の公約数であることは，図 2 の (i) 式,(ii) 式,(iii) 式を逆にたどることで確認できる[3]。また，最大であることは，6 よりも大きな 42 と 30 の公約数が存在するとして，(i) 式,(ii) 式,(iii) 式をこの順にたどれば，不合理が生じ，そのような公約数は存在しないことがわかる。

今，仮に 6 よりも大きな 42 と 30 の公約数 x があったとする。(i) 式をみれば，x は，左辺である 42 を割り切るのだから，右辺 $30 \times 1 + 12$ も割り切る。ところが，x は，42 と 30 の公

[3] この証明はほとんど明らかなので省略する。

約数であるゆえ30を割り切るのだから，12を割り切らねばならない。同様に，(ii) 式をみれば，xは左辺である30を割り切り，右辺の12を割り切るのであるから，xは6も割り切ることになる。ところが，xは，6よりも大きい整数であったから，このことは不合理である[4]。

これがもっとも素朴なユークリッドの互除法の理解であろう。図2の系列は，例えば，(ii) 式から始まったとみれば，30と12の最大公約数を求めるユークリッドの互除法とみれるし，(iii) 式から始まったとみれば，12と6の最大公約数を求めるユークリッドの互除法ともみれる。つまり，この考えで図2をみれば，ユークリッドの互除法は，$(42,30),(30,12),(12,6),(2,0)$というように，「減少していく同じ公約数をもった整数の組の系列」としてみることができる[5]。この系列の同値性を保証するのが次の補題である。

補題 1 （ユークリッドの互除法） $\mathcal{Z}$を整数全体の集合とする。$a_1, a_2(\neq 0) \in \mathcal{Z}$，ただし，$a_1 \geq a_2$とする。これに対して，$a_1$を$a_2$で整除したときの商を$q_1$，余りを$r_1$とする。数式を用いて表現すれば，

$$a_1 = a_2 q_1 + r_1, (q_1, r_1 \in \mathcal{Z}, 0 \leq r_1 \leq a_2) \tag{1}$$

となる。このとき，a_1とa_2の公約数全体の集合はq_1とr_1の公約数全体の集合と一致する。したがって，a_1とa_2の最大公約数はa_2とr_1の最大公約数に等しい。a_1とa_2の公約数全体の集合を(a_1, a_2)で表し[6]，a_2とr_1の公約数全体の集合を(a_2, r_1)で表すことにすると，

$$(a_1, a_2) = (a_2, r_1) \tag{2}$$

が成り立つ。

それでは，まずI段階として，集合(a_1, a_2)からどんな要素を取ってきても，その要素が集合(a_2, r_1)の要素であることを示そう。

$\forall x \in (a_1, a_2)$とする。xはa_1とa_2の公約数であるから，xはもちろんa_2の約数である。これを以下，記号$|$を使って$x|a_2$と表現することにしよう。$x \in (a_2, r_1)$を示すためには，後，$x|r_1$であることを示せばよい。r_1は式(1)を変形すると，

$$r_1 = a_1 - a_2 q_1 \tag{3}$$

と表せる。$x \in (a_1, a_2)$だから，$a_1 = kx, a_2 = lx$を満たす$k, l \in \mathcal{Z}$が存在する。これらを(3)式に代入すれば，

$$r_1 = kx - lxq_1 = x(k - lq_1) \tag{4}$$

この式(4)は$x|r_1$を示している。よって，$x \in (a_2, r_1)$が示された。

逆に，第II段階として，集合(a_2, r_1)からどんな要素を取ってきても，その要素が集合(a_1, a_2)の要素であることを示そう。

$\forall y \in (a_2, r_1)$とする。yはa_2とr_1の公約数であるから，もちろん$y|a_2$である。$y \in (a_1, a_2)$を示すためには，あと$y|a_1$を示せばよい。$y \in (a_2, r_1)$なので，$a_2 = mx, r_1 = ny$を満たす$m, n \in \mathcal{Z}$が存在する。これらを式(1)に代入すると，

$$a_1 = myq_1 + ny = y(mq_1 + n) \tag{5}$$

この式(5)は$y|a_1$を示している。よって，$x \in (a_1, a_2)$が示された。ゆえに，(2)式が成り立つことが示された。

3.2 一般化のアイディアとその証明

ユークリッドの互除法の一般化についての証明に入る前に，本稿で問題にしているユークリッドの互除法の一般化とは何を意味して

[4] ここで用いた証明方法は，ユークリッド原論第7巻命題2の証明と本質的に同じ考え方を用いている。

[5] これを図式的に表現したのが図3である。

[6] a_1とa_2の最大公約数を(a_1, a_2)と表すことがあるが，ここではa_1とa_2の公約数全体の集合を表すことにする。

いるのかということと，それを考えるに至った文脈について述べておくことにする。

ユークリッドの互除法は，上で述べてきたように，基本的には2つの数に対するアルゴリズムである。それを3つ以上の数について考えることは自然なことである。しかし，例えば，3つの数に対しては，ユークリッドの互除法を2回適用すればその最大公約数は求まる。したがって，実用的観点からみれば，これまで述べてきたユークリッドの互除法で十分である。実際，3つの数に対して，ユークリッドの互除法を2回適用するというアイディアは，ユークリッド原論の第7巻命題3の方法[11]そのものである。この方法は，4個以上の整数の場合にも原論第7巻命題2の原理を繰り返すことで対処しうることを示唆しているから，ここであえてユークリッドの互除法を一般化するとは一体どういうことなのか説明しなければならないであろう。

本稿で取り上げようとするユークリッドの互除法の一般化は，このような実用的な観点から生まれたものではない。むしろ，アルゴリズムの形式性から生まれたもの，その形式性の背後にある数の関係そのものへの関心から生まれたものといえるものである。

これを説明するために，ユークリッドの互除法のアルゴリズムを次のように図式化してみよう。

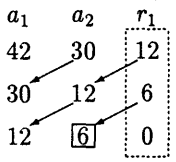

図 3: ユークリッドの互除法の図式化

この形式を拡張して，3つの整数に適用することを考えることは自然なことである。その際，問題となるのが第4番目の数をどのように決めるかである。2つの整数の場合には2つの整数のうち大きい整数を小さい整数で割った時の余りであった。3つの整数の場合，これに対応する数は何か?

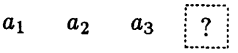

図 4: 第4番目の数は何か?

今，この3つの整数を $a_1, a_2, a_3 (\neq 0)$，ただし，$a_1 \geq a_2 \geq a_3$ とし，a_1 を a_2 で整除したときの余りを r_1，a_2 を a_3 で整除したときの余りを r_2 とする。結論からいえば，この第3番目の整数は，$r_1 + r_2$ になる。

3つの整数 a_1, a_2, a_3 をそれぞれ，42, 30, 24 とおいて，例証してみよう。

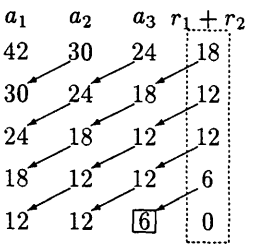

図 5: ユークリッドの互除法の図式化 (2)

この場合，$r_1 + r_2 = 0$ となったときの a_3 の位置にある数6が求める最大公約数である。

それでは，ユークリッドの互除法の拡張，3つの整数の場合の証明をすることにする。図5で示したこのアルゴリズムはまだ検討の余地を残している。このことは後で述べることにして，このアルゴリズムを支えている原理，つまり，上で述べた，2個の整数から成る同値な組の減少する系列が，3個の場合にも構成可能であることを示すことにする。そして，このアイディアを n 個の整数の場合に一般化することを試みることにする。

補題 2 （3つの整数の場合） $\mathcal{Z}$ を整数全体の集合とする。$a_1, a_2, a_3 (\neq 0) \in \mathcal{Z}$，た

だし，$a_1 \geq a_2 \geq a_3$。これに対して，a_1 を a_2 で整除したときの商を q_1，余りを r_1 とする。a_2 を a_3 で整除したときの商を q_2，余りを r_2 とする。数式を用いて表現すれば，

$$a_1 = a_2 q_1 + r_1, \quad (q_1, r_1 \in \mathcal{Z}, 0 \leq r_1 \leq a_2) \quad (6)$$

$$a_2 = a_3 q_2 + r_2, \quad (q_2, r_2 \in \mathcal{Z}, 0 \leq r_2 \leq a_3) \quad (7)$$

となる。このとき，r_1 と r_2 の和 r_1+r_2 を考える。このとき，a_1, a_2, a_3 の公約数全体の集合は a_2, a_3, r_1+r_2 の公約数全体の集合と一致する。a_1, a_2, a_3 の公約数全体の集合を (a_1, a_2, a_3) で表し，a_2, a_3, r_1+r_2 の公約数全体の集合を (a_2, a_3, r_1+r_2) で表すことにすると，

$$(a_1, a_2, a_3) = (a_2, a_3, r_1 + r_2) \quad (8)$$

が成り立つ。したがって，a_1, a_2, a_3 の最大公約数は，a_2, a_3, r_1+r_2 の最大公約数に等しい。

この補題を証明する前に，いくつかの簡単な変形規則とでもいうべきものを導入しておくことにする。

命題 2.1 $a, b, c \in \mathcal{Z}$ に対して，

$$(a, b, c) = ((a, b), c) = (a, (b, c))$$

が成り立つ。

命題 2.2 $a, b \in \mathcal{Z}$ に対して，

$$(a, b) = (b, a)$$

が成り立つ。a, b の公約数全体の集合は，b, a の公約数全体の集合と同じなので明らかである。同様に，$\mathcal{A}, \mathcal{B}$ をそれぞれ特定のいくつかの整数の公約数全体の集合とすると，

$$(\mathcal{A}, \mathcal{B}) = (\mathcal{B}, \mathcal{A})$$

が成り立つ。したがって，順序に関係なく入れ換えることができる。

命題 2.3 $a, b, c \in \mathcal{Z}$ に対して，

$$(a, b, c) = ((a, b), (b, c))$$

が成り立つ。なぜなら，$\forall x \in (a, b, c)$ とすると，$x|a, x|b, x|c$ であるから，$x|(a, b), x|(b, c)$ がいえる。ゆえに，$x \in ((a, b), (b, c))$。逆に，$\forall y \in ((a, b), (b, c))$ とすると，$y \in (a, b), y \in (b, c)$ だから，$y|a, y|b, y|c$ である。ゆえに，$y \in (a, b, c)$ が成り立つ。

命題 2.4 $\mathcal{A}, \mathcal{B}, \mathcal{C}$ をそれぞれ特定のいくつかの整数の公約数全体の集合とする。このとき，$\mathcal{A} = \mathcal{C}$ ならば，

$$(\mathcal{A}, \mathcal{B}) = (\mathcal{C}, \mathcal{B})$$

が成り立つ。公約数の集合として同じものを代入しているので明らか。

命題 2.5 $a, b \in \mathcal{Z}$ に対して，

$$(a, a + b) = (a, b)$$

が成り立つ。なぜなら，$\forall x \in (a, a+b)$ とすると，$x|a, x|a+b$ であるから，$a = xe, a+b = xf$ となる $e, f \in \mathcal{Z}$ が存在する。$a+b = xf$ の両辺から a を引き，$a = xe$ を代入すれば，$b = xf - a = xf - xe = x(f-e)$ となる。ゆえに，$x|b$。したがって，$x \in (a, b)$ である。逆に，$\forall y \in (a, b)$ とすると，$y|a, y|b$ であるから，$a = yg, b = yh$ となる $g, h \in \mathcal{Z}$ が存在する。これらを加えて変形すると，$a+b = yg+yh = y(g+h)$ となる。ゆえに，$y|a+b$。したがって，$y \in (a, a+b)$ である。

それでは，補題 2 の証明をすることにしよう。$\forall x \in (a_1, a_2, a_3)$ とする。このとき，$x \in (a_2, a_3, \alpha)$ すなわち，$x \in (a_2, a_3, r_1 + r_2)$ を示す。

命題 2.3 より，

$$(a_1, a_2, a_3) = ((a_1, a_2), (a_2, a_3)) \quad (9)$$

よって，$x \in ((a_1, a_2), (a_2, a_3))$。したがって，

$$x \in (a_2, a_3) \quad (10)$$

補題 1 より，$(a_1, a_2) = (a_2, r_1)$ (9) 式から $x \in (a_2, r_1)$ となるから，

$$x|r_1 \tag{11}$$

補題1より，$(a_2, a_3) = (a_3, r_2)$ (9)式から$x \in (a_3, r_2)$となるから，

$$x|r_2 \tag{12}$$

(11),(12)より，

$$x|(r_1, r_2) \tag{13}$$

したがって，$r_1 = xi, r_2 = xj$となる$i, j \in \mathcal{Z}$が存在する。辺々加えると，$r_1 + r_2 = xi + xj = x(i + j)$。ゆえに，

$$x|r_1 + r_2 \tag{14}$$

が成り立つ。

(10),(14)より，

$$x \in (a_2, a_3, r_1 + r_2) \tag{15}$$

逆に，$\forall y \in (a_2, a_3, r_1 + r_2)$とする。$(a_2, a_3, r_1 + r_2)$は，上述の変形規則を用いれば次のように変形することができる。

(命題2.1)より，

$$(a_2, a_3, r_1 + r_2) = ((a_2, a_3), r_1 + r_2) \tag{16}$$

(補題1; 命題2.4)より，

$$(a_2, a_3, r_1 + r_2) = ((a_3, r_1), r_1 + r_2) \tag{17}$$

(命題2.1)より，

$$(a_2, a_3, r_1 + r_2) = (a_3, (r_1, r_1 + r_2) \tag{18}$$

(命題2.5)より，

$$(a_2, a_3, r_1 + r_2) = (a_3, (r_1, r_2)) \tag{19}$$

(命題2.3)より，

$$(a_2, a_3, r_1 + r_2) = ((a_3, r_1), (r_1, r_2)) \tag{20}$$

したがって，$y \in (a_3, r_1), y \in (r_1, r_2)$。よって，$y|r_1$また，補題1から，$(a_2, a_3) = (a_3, r_1)$なので，$y \in (a_2, a_3)$。よって，$y|a_2$。補題1より$(a_1, a_2) = (a_2, r_1)$。ゆえに，$y \in (a_1, a_2)$，すなわち，$y|a_1$。

定理 （**一般化**）$\mathcal{Z}$を整数全体の集合とする。任意のn個の整数に対して，すなわち，例えば，$a_1, a_2, \cdots, a_n (\neq 0) \in \mathcal{Z}$，ただし，$a_1 \geq a_2 \geq \cdots \geq a_n$とし，$a_1$を$a_2$で整除したときの余りを$r_1$，$a_2$を$a_3$で整除したときの余りを$r_2$，同様に，$a_{n-1}$を$a_n$で整除したときの余りを$r_{n-1}$とする。このとき，$R_{n-1} = r_1 + r_2 + r_3 + \cdots + r_{n-1}; (n \geq 2)$と表せば，

$$(a_1, a_2, \cdots, a_n) = (a_2, a_3, \cdots, a_n, R_{n-1}) \tag{21}$$

が成り立つ。したがって，$a_1, a_2, \cdots, a_n$の最大公約数は，$a_2, a_3, \cdots, a_n, R_{n-1}$の最大公約数に等しい。

$n(\geq 2)$に関する帰納法で証明する。

(i)$n = 2$のとき，つまり，2つの整数に対して，式(21)は次のようになる。

$$(a_1, a_2) = (a_2, R_1) \tag{22}$$

ここで，$R_1 = r_1$であるから，これは既に証明した補題1（ユークリッドの互除法）に他ならない。したがって，$n = 2$のとき，式(21)は成り立つ。

(ii)$n = k$のとき，つまり，k個の整数に対して，式(21)は成り立つと仮定する。すなわち，$R_{k-1} = r_1 + r_2 + r_3 + \cdots + r_{k-1}$と表せば，

$$(a_1, a_2, \cdots, a_k) = (a_2, a_3, \cdots, a_k, R_{k-1}) \tag{23}$$

が成り立つと仮定する。

このとき，$n = k + 1$のときも成り立つことを示す。すなわち，$R_k = r_1 + r_2 + \cdots + r_k$と表せば，

$$(a_1, a_2, \cdots, a_{k+1}) = (a_2, a_3, \cdots, a_{k+1}, R_k) \tag{24}$$

が成り立つことを示す。

今，簡単のために$(a_1, a_2, \cdots, a_{k+1}) = X$とし，$(a_2, a_3, \cdots, a_{k+1}, R_k) = Y$としておくことにする。

まず第I段階として証明すべきことは，$\forall x \in X$とすると必ず$x \in Y$となることである。そのためには，$x|R_k$を示せば十分である。なぜなら，XとYの違いはa_1とR_kのところだけであることに注意すると，$x \in X$ということ自体によって，本来示さなければならない諸関係である，$x|a_2, x|a_3, \cdots, x|a_{k+1}$が既に示されていることになっているからである。つまり，残りの関係$x|R_k$が成り立つことさえ示せば，xは，Yを構成している$k+1$個の整数すべての約数であることを示すことができるので，$x \in Y$が示せるということである。

まず，Xを帰納法の仮定を用いて変形すると，すなわち，命題2.4を使って，Xの中の一部の整数の組$a_1, a_2, \cdots, a_k$を(23)式が示唆するその組と全く同じ公約数をもつ整数の組$a_2, a_3, \cdots, a_k, R_{k-1}$で置き換えると，

$$X = (a_2, a_3, \cdots, a_k, R_{k-1}, a_{k+1}) \tag{25}$$

したがって，

$$x|R_{k-1} \tag{26}$$

R_kは，定義から

$$R_k = R_{k-1} + r_k \tag{27}$$

また，r_kは，a_kをa_{k+1}で割ったときの余りであるから，補題1(ユークリッドの互除法)より，

$$(a_k, a_{k+1}) = (a_{k+1}, r_k) \tag{28}$$

が成り立つ。$x \in X$なので，当然，$x \in (a_k, a_{k+1})$である。したがって，(28)式より，$x \in (a_{k+1}, r_k)$。したがって，

$$x|r_k \tag{29}$$

(26), (27), (29)から，

$$x|R_k \tag{30}$$

よって，$x \in Y$。

次に，第II段階として，逆に，$\forall y \in Y$とすると必ず$y \in X$となることを示す。そのためには，上で述べたのとちょうど同じ理由から，$y|a_1$を示せば十分であることがわかるであろう。そして，$y|a_1$を示すためには，結局，$y|r_1$を示せばよいことも示唆されるであろう。なぜなら，$y \in Y$であるから，$y|a_2$であり，補題1から$(a_1, a_2) = (a_2, r_1)$が成り立つことがわかっているので，この関係を用いると$y \in (a_1, a_2)$であること，すなわち，$y|a_1$を示すことができるからである。

帰納法の仮定により，k個の整数に対して定理は成り立っている[7]ので，

$$(a_2, a_3, \cdots, a_{k+1}) = (a_3, a_4, \cdots, a_{k+1}, r_2 + r_3 + \cdots + r_k) \tag{31}$$

が成り立つ。

この関係をYに適用すると，すなわち，命題2.4を使って，Yの中の一部の整数の組$a_2, a_3, \cdots, a_{k+1}$を(31)式が示唆するその組と全く同じ公約数をもつ整数の組$a_3, a_4, \cdots, a_{k+1}, r_2 + r_3 + \cdots + r_k$で置き換えると，

$$Y = (a_2, a_3, \cdots, a_{k+1}, R_k)$$

[7]定理は，(24)式そのものではなく，(24)式が示唆する関係の成立を主張していることに注意。その関係とは，『n個の整数があって，それを大きい順番に並べ替える。大きい整数をその次に大きい整数でわり算を次々に行う。n個の整数の場合，$n-1$回のわり算をすることになる。その結果生じる$n-1$個の余りの合計をR_{n-1}すると，n個の整数の公約数全体の集合と，この集合から最大の数を余りの合計R_{n-1}で置き換えた集合の公約数全体の集合は一致する』ということである。したがって，ここでの帰納法の仮定である，(23)式は，任意のk個の整数に対して，それらの間に，(23)式とともに示されている関係が成立してさえいれば，(23)式は成立するという意味である。言うなれば，式そのものは，定理の一つの具体的表現であり，一つの例であるということである。

$$= (a_3, a_4, \cdots, r_2 + r_3 + \cdots + r_k, R_k) \tag{32}$$

ここで，(32) 式の後半の式の中の関係 $r_2 + r_3 + \cdots + r_k, R_k$ に注目すると，$R_k = r_1 + r_2 + \cdots + r_k$ であるから，$A = r_2 + r_3 + \cdots + r_k$ とおけば，$r_2 + r_3 + \cdots + r_k, R_k$ は，$A, r_1 + A$ と書くことができる。これを命題 2.5 を用いて変形すると，

$$(A, r_1 + A) = (A, r_1) \tag{33}$$

となる。すなわち，(32) 式の後半の式の中の関係が示唆する公約数全体の集合 $(r_2 + r_3 + \cdots + r_k, R_k)$ は，(A, r_1) と等しい。したがって，命題 2.5 を適用して，(32) 式の後半の式の中の関係 $r_2 + r_3 + \cdots + r_k, R_k$ を A, r_1 で置き換えると，

$$Y = (a_3, a_4, \cdots, a_{k+1}, A, r_1) \tag{34}$$

(34) 式は，$y | r_1$ であることを示している。

4 おわりに

このユークリッドの互除法の一般化は，その意味や実用的な観点から生まれたというよりも，形式性，とりわけ，ユークリッドの互除法を図 3 のような図式でそのアイディアを表現したことが契機となっていた。ユークリッドの互除法のアイディアを図式で表現することによって，形式が先行し，ユークリッドの互除法が持っているもともとの意味から離れる結果となり，その図式の中にある関係そのものが問題となったといえそうである。$r_1 + r_2$ を第 4 番目の数にするというようなアイディアは，意味を考えている間には思いもつかないかもしれない。

本稿でみてきたように，ある文脈を与えれば，非常に自然で興味深いと思われるこのユークリッドの互除法の一般化が，これまであまり問題にされてこなかったとすれば，その理由を考えることは，数学と人間性との関連を考える上で役立つように思われる。それは，数学的関係とその応用可能性との関係であり，おそらく，この一般化が，最大公約数を求めるという実用的な目的にとって，従来のユークリッドの互除法の繰り返しの適用以上の効果をもっているようには思われないからであろう。逆に，それ自身興味深いというだけでは知識として生き残るには少し弱いのかもしれない。

ユークリッドの互除法の場合は，余りが必ず除数よりも小さくなるので，最初の 2 数が与えられたときに大小の関係を意識してさえいれば後は大小関係を気にする必要はない。ところが，ここで述べてきたユークリッドの互除法の一般化の場合には，出てきた余りを足すという操作をするので，この和が除数よりも大きくなってしまうということが起こりうるのである。例えば，3 つの整数 48,34,20 を例にとって考えてみよう。

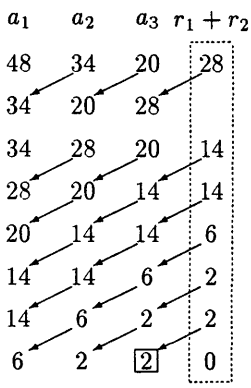

図 6: 並べ換えが必要な例

この場合には，図 6 の最初の段の余りの和 $r_1 + r_2 = 28$ が，その同じ段の整数 $a_3 = 20$ よりも大きくなってしまっている。したがって，2 段目において大きい順に並べ換えて (命題 2.2)，3 段目から新たにユークリッドの互除法の一般化の原理を適用すればよい。

さらに，一般化の準備として行った補題 2 の証明や幾つかの命題には，その後の定理

にとって無駄なことも含まれているし，ほとんど自明に思われる。しかし，形式的な変形をしようとしたとき，少なくとも，私自身がその意味に返り，変形の前後で同値関係が保持されているかどうかを確認した事柄であった。一方，このような反省によって，今まで気づかなかった重要な関係を意識することになった。例えば，命題2.5として定式化した関係はその一例である。これは，ある意味で，ユークリッドの互除法の特殊化であるともいえるし，2数の最大公約数は2数の差の約数であるというきわめて単純な関係をも示唆している[8]。

ユークリッドの互除法は除法であるが，この除法を累差と解釈すれば，命題2.5の減数と差の関係は，ユークリッドの互除法における除数と余りの関係に対応している。そして，命題2.5はユークリッドの互除法の途中の段階であり，この段階においても上で述べたような同値性が保たれているということである。この関係に気づくことは，証明において必要であっただけではなく，私にとっては，数に対する感覚がより豊かになっていることを実感しうるものであった。

例えば，この関係に気づいていれば，286と284の最大公約数は286と284の差である2の約数であるともみれるし，284と2との最大公約数と等しいともみれる。2の約数は1と2である。286と284が偶数であるから，最大公約数は2であることが一瞬にしてわかるからである[9]。

[8]ある整数論のテキスト[12]では，$(a,b)=(a-b,b)$として表現されている。ここで，(a,b)はa,bの最大公約数を表している。これは勿論，本稿で述べた命題2.5と同値であるが，この表現の方が，ここで述べた差の関係を明確に表現しているといえよう。

[9]別の例[13]として，例えば，$5^{20}+8$と$5^{20}+3$の最大公約数について考える場合でも，同様に，その差を考えると5であり，最大公約数の候補は5の約数である1と5に限られる。ところが，5で割り切れないことは明らかであるから，結局，これらは互いに素であることがわかる。

このユークリッドの互除法の一般化が中学校における「課題学習」などの生徒たちのための教材として仕立て直すことが可能であるかどうかはまだ検討していない。これは今後の課題とし，できればゼミの学生や院生，数学教育の自主サークルであるΣ会の先生方と一緒に考えていきたいと思っている。

引用文献

1) 平林一栄 (1994a). 算数指導が楽しくなる小学校教師の数学体験. 黎明書房, 13-14 頁.

2) 古藤　怜, 上越数学教育研究会Σ会 (1991). 算数・数学科における *Do Math* の指導. 東洋館出版社.

3) ユークリッド (1971). ユークリッド原論 (中村幸四郎 他訳). 共立出版, 151 頁.

4) 彌永昌吉・伊東俊太郎・佐藤徹 (1979). 数学の歴史 1 ギリシャの数学. 共立出版, 47-48 頁.

5) 平林一栄 (1994b). 算数教育における数学史的問題 —「量」に関連して—. 皇學館大學講演叢書第七十五輯, 33–39 頁.

6) 岩崎　浩 (1998). 具体的教材（題材）の陶冶価値を検討することの意味：非通約量（無理数）の発見に対するプラトンの見解. 一般教科教育学研究会編, 一般教科教育学序説, 大学教育出版.

7) 文部省 (1989). 中学校指導書　数学編. 大阪書籍, 152 頁.

8) 川口　延 他 (1992). 中学校数学 3. 学校図書.

9) 文部省 (1989). 小学校指導書　算数編. 大阪書籍, 212 頁.

10) 一松　信 他 (1995). 小学校算数 5 年下. 学校図書.

11) ユークリッド (1971). 前掲書. 152–153 頁.

12) 山本芳彦 (1996). 数論入門 1 岩波講座 現代数学への入門 4. 岩波書店, 19 頁.

13) 山本芳彦 (1996). 同掲書. 20 頁.