新課程の内容「整数の性質」についての一考察

―わかりやすいユークリッドの互除法の証明を求めて―

西元(にしもと) 教善(のりよし)

§0. はじめに

次期教育課程の数学Aでは「整数の性質」が新内容として導入され，その中には「**ユークリッドの互除法**」を扱うようになっている。指導要領の中では「整数の除法の性質に基づいて，ユークリッドの互除法の仕組みを理解し……」とある。互除法の「仕組み」という文言があるから，具体例でその仕組みを理解することも考えられるが，基本的にはその証明が出てくるはずである。

証明方法は多様である。しかし，生徒にとって受け入れやすい「わかる」証明による「仕組みの理解」でなければならない。

§1. 互除法の証明(証明の要点)

周知のとおり，ユークリッドの互除法とは，『a，b を自然数とするとき，a を b で割ったときの商を q，余りを r $(0\leqq r<b)$ とするとき，a と b の最大公約数と，b と r の最大公約数は等しい』というものである。

証明では，「被除数 a と除数 $\boldsymbol{b}$ の最大公約数」と「除数 $\boldsymbol{b}$ と余り r の最大公約数」が等しいことを，どのようにして，生徒にとって受け入れやすい「わかる」説明をするかが要点である。

なお，「被除数 a と除数 $\boldsymbol{b}$ の最大公約数」とか「除数 $\boldsymbol{b}$ と余り r の最大公約数」というような表現では冗長になるので，説明の簡便さのために，自然数 m，n の最大公約数を $(\boldsymbol{m},\ \boldsymbol{n})$，最小公倍数を $[\boldsymbol{m},\ \boldsymbol{n}]$，さらには m は n を割り切る(つまり，m は n の約数である，あるいは，n は m の倍数)ことを $\boldsymbol{m}|\boldsymbol{n}$ を表すものとする。

以前では，中学校で最大公約数，最小公倍数をG.C.M, L.C.M といった記号で表していたが，最近では扱っていない。それどころか最大公約数，最小公倍数という用語さえ発展的な扱いである。最大公約数を g，最小公倍数を l と表してもそのアルファベットの持つ意味がわからないのは当然かも知れない。記号 $(m,\ n)$，$[m,\ n]$ でわかりづらいようであれば，**g.c.m.**$(\boldsymbol{m},\ \boldsymbol{n})$，**l.c.m.**$(\boldsymbol{m},\ \boldsymbol{n})$ というような記号でも導入すればよい。

さて，早速ではあるが，これらの記号を使って表せば，次の3つの証明が考えられる。

> **証明1**　$\{n|n|a$ かつ $n|b\}=\{n|n|b$ かつ $n|r\}$ を示すことで，$[a,\ b]=[b,\ r]$ を示す。
> **証明2**　$[a,\ b]\geqq[b,\ r]$ かつ $[a,\ b]\leqq[b,\ r]$ を示すことで，$[a,\ b]=[b,\ r]$ を示す。
> **証明3**　$[a,\ b]|[b,\ r]$ かつ $[b,\ r]|[a,\ b]$ を示すことで，$[a,\ b]=[b,\ r]$ を示す。

<u>証明1の要点</u>

$A=\{n|n|a$ かつ $n|b\}$，$B=\{n|n|b$ かつ $n|r\}$ とする。$n\in A$ とすると，n は a と b の公約数であり，当然 b の約数である。すると，$r=a-bq$ より，r の約数でもあるから，n は b と r の公約数である。

つまり，$n\in B$ となるから，$A\subset B$ ……①

また，$n\in B$ とすると，n は b と r の公約数であり，当然 b の約数である。すると $a=bq+r$ より，a の約数でもあるから，n は a と b の公約数である。

つまり，$n\in A$ となるから，$B\subset A$ ……②

したがって，①，②より $A=B$

$n|a$ かつ $n|b \Longleftrightarrow n$ は a と b の公約数

$n|b$ かつ $n|r \Longleftrightarrow n$ は b と r の公約数

であるから，結局，

$\{n|n$ は a と b の公約数$\}=\{n|n$ は b と r の公約数$\}$

したがって，左の公約数で最大である $[a,\ b]$ と右の公約数で最大である $[b,\ r]$ は一致する。

あるいは，これは，

$\{n|n$ は a と b の公約数$\}=\{n|n$ は b と r の公約数$\}$

さらには，$\{n|n|[a,\ b]\}=\{n|n|[b,\ r]\}$ と表した方がよいかもしれない。

証明 2 の要点

$[a,\ b]$ は b の約数であり，$r=a-bq$ より $[a,\ b]$ は r の約数でもあるから，$[a,\ b]$ は b と r の公約数である。

公約数は最大公約数以下であるから，

$[a,\ b]\leqq[b,\ r]$ ……③

また，$[b,\ r]$ は b の約数であり，$a=bq+r$ より $[b,\ r]$ は a の約数でもあるから，$[b,\ r]$ は a と b の公約数である。

よって，同じ理由から，$[a,\ b]\geqq[b,\ r]$ ……④

③と④より，$[a,\ b]=[b,\ r]$ である。

証明 3 の要点

a と b の最大公約数 $[a,\ b]$ は b の約数であり，$r=a-bq$ より $[a,\ b]$ は r の約数でもあるから，$[a,\ b]$ は b と r の公約数である。

公約数は最大公約数の約数であるから，

$[a,\ b]|[b,\ r]$ ……⑤

また，$[b,\ r]$ は b の約数であり，$a=bq+r$ より $[b,\ r]$ は a の約数でもあるから，$[b,\ r]$ は a と b の公約数である。

よって，同じ理由から，$[b,\ r]|[a,\ b]$ ……⑥

⑤と⑥より，$[a,\ b]=[b,\ r]$ である。

§2. 証明 1，2，3 の比較

証明 1 について

証明 1 は，a と b の任意の公約数が b と r の公約数になることから，

$$\{a \text{ と } b \text{ の公約数}]\subset[b \text{ と } r \text{ の公約数}]$$

であることを示し，また，逆に，b と r の任意の公約数が a と b の公約数になることから，

$$\{b \text{ と } r \text{ の公約数}\}\subset\{a \text{ と } b \text{ の公約数}\}$$

を示すことによって，

$$\{a \text{ と } b \text{ の公約数}\}=\{b \text{ と } r \text{ の公約数}\}$$

を導き，集合として一致しているから，それぞれの最大公約数は一致するという論法である。

なぜ，$n\in A$ と表現をしたのかといえば，2 つの集合 A，B が等しいこと $(A=B)$ は，「$A\subset B$ かつ $B\subset A$」であることであり，$A\subset B$ を示すには，「$x\in A \Longrightarrow x\in B$」を示せばよいという背景があるからである。

また，集合として等しいことは，2 つの集合のすべての要素が一致していることから，それぞれにある最大公約数 $[a,\ b]$，$[b,\ r]$ が一致することを理解していなければならない。

いずれにしても，集合の基礎知識をもっていることが前提である。

証明 2 について

証明 2 では，「最大公約数はそれぞれの数の（共通の）約数であること」を押さえておかなければならない。

つまり，a と b の最大公約数は，b の約数であること，$r=a-bq$ より r の約数でもあることを理解しなければならない。

よって，a と b の最大公約数は，b と r の公約数，したがって，b と r の最大公約数の約数であり，したがって，その値はそれ（最大公約数）以下である。ここで，

$$[a,\ b]\leqq[b,\ r]$$

という大小関係がいえるのである。

あとは，同様の展開で，その逆 $[a,\ b]\geqq[b,\ r]$ がいえる。よって，$[a,\ b]=[b,\ r]$ となるわけである。

最大公約数は，最大公約数を考えているそれぞれの数の「約数」という，いわば一旦最大からの格下げをして，一致を示したい「最大公約数の約数」であることを示し，その値がそれ以下であることをいう。次に，お互い様ということで，今度はそれが相手の最大公約数以下になることを示す。

また，そこには，

$$m=n \Longleftrightarrow m\leqq n \text{ かつ } m\geqq n$$

という関係が押さえられていなければならない。

証明 3 について

証明 3 は，証明 2 と同じ流れの中で，大小関係ではなく，整除関係に持ち込むものである。

ここでは，自然数 m，n において，

$$m=n \Longleftrightarrow m|n \text{ かつ } n|m$$

という関係が押さえられていなければならない。

これも証明 2 と同様に，生徒にとっては盲点を突く印象を与えるかも知れない。

§3. 証明1，2，3の背景

ここで，この3つの証明の背景を分類してみると，次のようなことがわかる。

証明1　包含関係と一致

$$A \subset B \text{ かつ } B \subset A \Longleftrightarrow A=B$$

証明2　大小関係と一致

$$a \leqq b \text{ かつ } a \geqq b \Longleftrightarrow a=b$$

証明3　整除関係と一致

$$a|b \text{ かつ } b|a \Longleftrightarrow a=b$$

これらの基盤をしっかりさせておかなければ，折角の説明も生徒の理解にとってはわかりにくいものになる。

§4. 4つ目の証明(ストレートな証明)

この辺りの議論は，やはり生徒の苦手とするところである。しかし，もう少し，生徒にとってわかりやすい説明はないのだろうか？

ここで，生徒にとってわかりやすいのは，やはり「a と b の最大公約数」＝「b と r の最大公約数」が，直接「＝」で説明させるものではなかろうか，と考える。

生徒には，「＝」は「＝」で示すものという思いがあるからである。恐らく，不等式「≧」かつ「≦」で「＝」を示すという発想は稀であろう。

つまり，「G が b と r の最大公約数」とすると「a と b の最大公約数は G」が直接に説明されるものであると思う。そこで，次のような4番目の証明を考える。

証明4　$[a, b]=[b, r]$ をストレートに証明 $a=bq+r\ (0 \leqq r<b)$　…①

①において，b と r の最大公約数を G とすると，$b=Gb'$ …②，$r=Gr'$ (b' と r' は互いに素)と表されるので，これより①は，

$$a=G(b'q+r') \quad \cdots ③$$

と表せる。

b' と $b'q+r'$ の最大公約数を $\boldsymbol{g}$ とすると，

$$b'=\boldsymbol{g}c \ \cdots ④, \quad b'q+r'=\boldsymbol{g}d \ \cdots ⑤$$

(c と d は互いに素 …⑥)

と表せる。

すると，④と⑤より　$\boldsymbol{g}cq+r'=\boldsymbol{g}d$

よって，$r'=\boldsymbol{g}(d-cq)$ …⑦

④，⑥より，g は b' と r' の公約数になる。

ここで，b' と r' は互いに素(公約数は1)であるから，$\boldsymbol{g}=1$

よって，④と⑤により，$b'=c$，$b'q+r'=d$ であり，⑥からは b'，$b'q+r'$ は互いに素である。②と③により，G は a と b の最大公約数である。

よって，a と b，b と r の最大公約数は等しい。

さて，この証明では，2数 a，b について，

$a=Ga'$，$b=Gb'$ (a' と b' は互いに素) $\Longleftrightarrow [a, b]=G$

互いに素 $\Longleftrightarrow$ 最大公約数が1 $\Longleftrightarrow$ すべての約数が1

であることさえ押さえておけばよいので，証明1～3よりは(生徒にとっても)わかりやすいと思われる。というのも，他の予備知識が不要であるからである。

§5. 互除法の実際的運用について

さて，ここまでユークリッドの互除法の証明を中心に考察したが，次に実用面を考察する。

a，b ($a>b$) を自然数とし，a を b で割ったときの商を q，余りを r ($0<r<b$) とする。

① $r=0$ ならば，$a=bq$ ($q \in N$) となるので，$(a, b)=b$ である。

② $r>0$ ならば，b を r で割ったときの商を q，余りを r_1 ($0 \leqq r_1<r$) とする。

$r_1=0$ ならば，$b=rq$ ($q \in N$) となるので，$(b, r)=r$ である。すると，ユークリッドの互除法から $(a, b)=(b, r)=r$

③ $r_1>0$ ならば，r を r_1 で割ったときの商を q_2，余りを r_2 ($0 \leqq r_2<r_1$) とする。

$r_2=0$ ならば，$r=r_1q_1$ ($q_1 \in N$) となるので，$(r, r_1)=r_1$ である。すると，ユークリッドの互除法から

$$(a, b)=(b, r)=(r, r_1)=r_1$$

………

これを一般化する。

自然数 n_0，自然数 r_k ($k=1, 2, 3, \cdots, n_0+2$) が，次の条件を満たすとする。

① $r_k>r_{k+1}$ ($k=1, 2, 3, \cdots, n_0+1$)

② r_k を r_{k+1} で割ったときの余りは，r_{k+2} ($0<r_{k+2}<r_{k+1}$ ($k=1, 2, \cdots, n_0$)，r_k を r_{k+1} で割ったときの商を q_k ($\in N$) とすると，$r_k=r_{k+1}q_k+r_{k+2}$)

③ r_{n_0+1} を r_{n_0+2} で割ったときの商を q_{n_0+1} ($\in N$)，余りを r_{n_0+3} とするとき，$r_{n_0+3}=0$ (つまり，r_{n_0+1}

$=r_{n_0+2}\,q_{n_0+1}$，すなわち，$r_{n_0+2}\,|\,r_{n_0+1}$)

このとき，③より，$(r_{n_0+1},\ r_{n_0+2})=r_{n_0+2}$ である。

すると，ユークリッドの互除法によって，

$(r_1,\ r_2)=(r_2,\ r_3)=\cdots=(r_{n_0+1},\ r_{n_0+2})=r_{n_0+2}$

$r_1=a$，$r_2=b$，$r_3=r$，$q_1=q$ とすれば，この場合では，$(a,\ b)=r_{n_0+2}$ ということになる。

なお，このように有限回で可能であるのは，余りについて，$0\leqq r_{k+1}<r_k\leqq r$ であることによる。

つまり，ユークリッドの互除法を有限回繰り返せば，必ず（余り）=0 となり，その直前の余り（≠0）が最初の 2 数の最大公約数である。

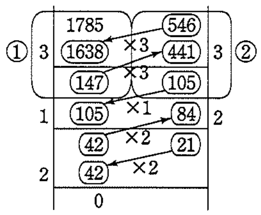
§6. 互除法による具体的計算

では，最後に互除法で具体的に 2 数の最大公約数を求めてみよう。

$a=1785$，$b=546$ とする。

	1785	546	
3	1638	441	3
	147	105	
1	105	84	2
	42	21	
2	42		
	0		

さて，この図の意味を考えてみよう。



① 1785 を 546 で割ると，商は 3 で余りは 147

つまり，1785=546×3+147

次に，② 546 を 147 で割ると，商は 3 で余りは 105　つまり，546=147×3+105

さらに，147 を 105 で割ると，商は 1 で余りは 42

つまり，147=105×1+42

さらに，105 を 42 で割ると，商は 2 で余りは 21

つまり，105=42×2+21

最後に，42 を 21 で割ると，割り切れて，商は 2

先程，見たように，割り切れる直前の余りがこの 2 数の最大公約数であるから，この場合は 21 である。実際，

$a=1785=3\times5\times7\times17$

$b=\ 546=2\times3\times7\times13$

である。また，この場合，

$(1785,\ 546)=(546,\ 147)=(147,\ 105)$
$=(105,\ 42)=(42,\ 21)=21$

ということである。

では，これを一般化して表してみよう。

	r_1	r_2	
q_1	r_2q_1	r_3q_2	q_2
	r_3	r_4	
q_3	r_4q_3	r_5q_4	q_4
	r_5	r_6	
	……		
q_{n_0}	$r_{n_0+1}q_{n_0}$	$r_{n_0+2}q_{n_0+1}$	q_{n_0+1}
	r_{n_0+1}	r_{n_0+2}	
q_{n_0+2}	$r_{n_0+3}q_{n_0+2}$		
	$r_{n_0+4}=0$		

図の左右にあるのは，商 q_k である。

§7. おわりに

『互除法』とはうまいネーミングである。まさしく，お互いを割ってその余りを直前の余りで割って…という繰り返しである。互除法はそのアルゴリズムを表しているわけであるが，なぜこのような方法で最大値が求められるかという証明と実用面としての方法の理解が求められる。ただ単に，こういうやり方ですれば求められますといった how to だけでなく，reason why を大切にしたい。

整数は魅力のある分野である。イギリスの数学者ハーディーは，初等整数論は早期数学教育にとって最適の教材の一つであると言っている。その理由は，予備知識をあまり必要としないこと，親しみやすいこと，推論の過程が単純なこと，好奇心に訴えやすいことからである。

課題学習も新教育課程では導入されるが，グループ学習等で適切に指導すれば，数学力の向上が十分に期待できる。そのためにも事前に研究や試みの実践をする必要があると思う。

（山口県立岩国高等学校）