ユークリッドの互除法を理解しよう

札幌創成高等学校

外山　尚生

§０　はじめに

　ユークリッドの互除法は２数の最大公約数を求めたり、一次不定方程式の整数解を求めるのにとても便利な計算方法である。しかし、ユークリッドの互除法の意味を理解しようとすると結構難しい。ここではユークリッドの互除法を具体例を考えながらユークリッドの互除法の意味を理解したい。

§１　ユークリッドの互除法

a と b の最大公約数を $gcd(a,b)$ と書くことにする。

例　12 と 18 の最大公約数は 6 であるから、 $gcd(12,18)=6$

１．１　ユークリッドの互除法

ユークリッドの互除法は次の性質が根拠となっている。

[定理１．１]

自然数 a 、 b について a を b で割ったときのあまりを r とすると $gcd(a,b)=gcd(b,r)$

例　391 を 299 で割った商は１、余りは 92 であるから $gcd(391,299)=gcd(299,92)$ が成り立つ。

注　実際、 $gcd(391,299)=23$ 、 $gcd(299,92)=23$ であるから成り立つ。

まずは定理１．１を証明しよう。

定理１．１を証明するためには次の２つを証明すればよい。

（Ⅰ） $gcd(a,b)$ は b,r の公約数である。 （Ⅱ） $gcd(a,b)=gcd(b,r)$ である。

$gcd(a,b)=m$ とおく。

a を b で割った商を q 、あまりを r とすると $a=bq+r$ より $r=a-bq$

$gcd(a,b)=m$ より $a=ma'$ 、 $b=mb'$ とおくと $r=ma'-mb'q=m(a'-b'q)$ より m は r の約数であるから、 m は b,r の公約数である。（Ⅰの証明終わり）

$gcd(b,r)=n$ とおく。

m は b,r の公約数であるから $m\leqq n$ …①がなりたつ。

$gcd(b,r)=n$ より $b=nb'$ 、 $r=nr'$ とおくと $a=bq+r=nb'q+nr'=n(b'q+r')$ より n は a の約数であるから、 n は a,b の公約数である。

よって $n\leqq m$ …②が成り立つ。

①②より $n=m$ である。（Ⅱの証明終わり）

しかしこの証明ではいまいち定理１．１のもつ意味が理解できない。そこで、定理１．１を帯分数と約分の視点から考えてみよう。

１．２　帯分数と約分の視点から考える

例えば仮分数 $\dfrac{391}{299}$ を考える。

$\dfrac{391}{299}$ は 391 と 299 の最大公約数である 23 で約分して $\dfrac{391}{299}=\dfrac{17}{13}$ と約分できる。

ところで $\dfrac{391}{299}$ は $1\dfrac{92}{299}$ と帯分数で表すことができる。ここで $\dfrac{92}{299}$ に注目しよう。

$\dfrac{391}{299}$ は 23 で約分できるのだから、 $1\dfrac{92}{299}$ も 23 で約分できることは感覚的にわかる。

（実際 $1\frac{92}{299}=1\frac{4}{13}$ である）

ここから、 $gcd(391,299)=gcd(299,92)$ であることがわかる。

一般化すると a を b で割った商を q 、余りを r とすると

$\frac{a}{b}=q\frac{r}{b}$ であるから、約分できる数を考えると $gcd(a,b)=gcd(r,b)$ であることは感覚的に理解できる。

§２　ユークリッドの互除法と最大公約数

２．１　ユークリッドの互除法と最大公約数

ユークリッドの互除法を繰り返すことで最大公約数を簡単に求めることができる。

例えば391 と 299 の最大公約数を求めよう。

$391 \div 299 = 1$あまり92

$299 \div 92 = 3$あまり23

$92 \div 23 = 4$あまり0

よってユークリッドの互除法より $gcd(391,299)=gcd(299,92)=gcd(92,23)=23$

ユークリッドの互除法を続けていって、あまりが 0 になったときの割る数が最大公約数となる。

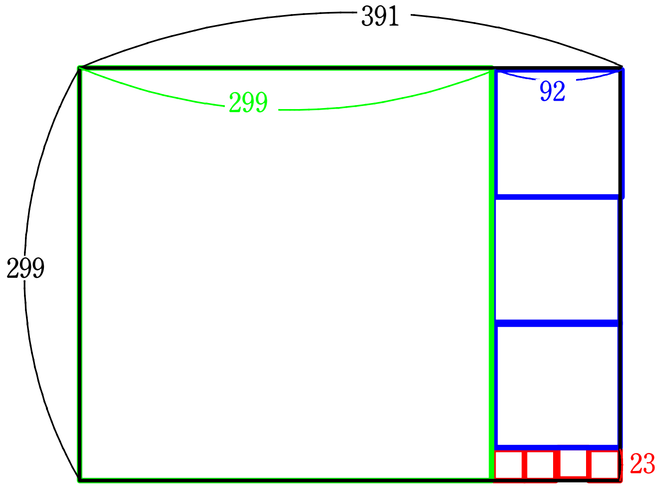
これを計算によって表すと次のようになる。

$$
\begin{array}{r}
1 \\
299\overline{)\,391} \\
\underline{299} \\
92
\end{array}
\qquad
\begin{array}{r}
3 \\
92\overline{)\,299} \\
\underline{276} \\
23
\end{array}
\qquad
\begin{array}{r}
4 \\
23\overline{)\,92} \\
\underline{92} \\
0
\end{array}
$$

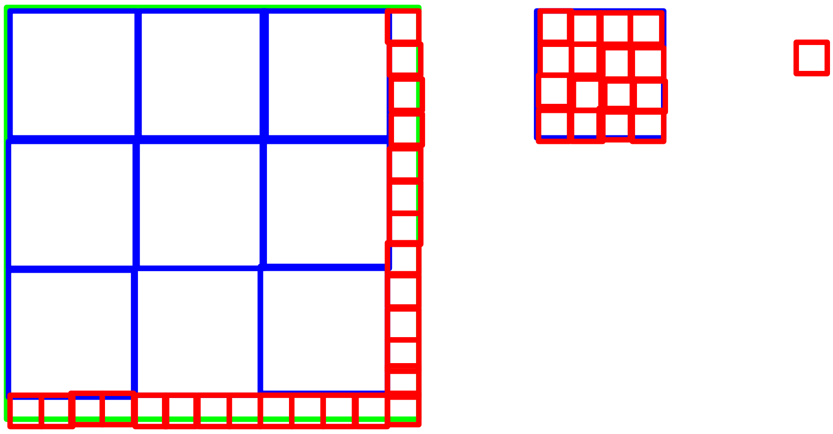
２．２　図形的解釈

長方形に正方形を敷き詰めることを考える。

例えば、 391 と 299 の長方形を考える。ここにいろいろな大きさの正方形を敷き詰める。正方形の数をできるだけ少なくするには次のように敷き詰めるとよい。



ここで緑の正方形は青と赤の正方形、青の正方形は赤の正方形で敷き詰めることができる。



ここから 391 と 299 はどちらも 赤の正方形の一辺の長さである23で割り切れることがわかる。

つまり 391 と 299 の最大公約数は 23 である。

２．３　帯分数と約分の視点から考える

　分数について、次の２つの性質は成り立つことは理解できる。

［性質１］　仮分数と帯分数の分数部分は同じ数で約分できる。
［性質２］　分数の分母と分子を入れ替えても同じ数で約分できる。

性質１は１．２で述べた内容である。性質２は明らかであろう。

２つの性質を繰り返すことによって最大公約数を求めることができる。

例えば $\frac{391}{299}$ を考える。

$\frac{391}{299}=1\frac{92}{299}$ より $\frac{391}{299}$ と $\frac{92}{299}$ は同じ数で約分できる（性質１）。

$\frac{92}{299}$ と $\frac{299}{92}$ は同じ数で約分できる（性質２）。

$\frac{299}{92}=3\frac{23}{92}$ より $\frac{299}{92}$ と $\frac{23}{92}$ は同じ数で約分できる（性質１）。

$\frac{23}{92}$ と $\frac{92}{23}$ は同じ数で約分できる（性質２）。

$\frac{92}{23}=\frac{4}{1}$ より「約分できる同じ数」は 23 である。

§３　ユークリッドの互除法と一次不定方程式の解

３．１　一次不定方程式の解

方程式 $177x-52y=1$ を満たす整数 (x,y) の組を１つ求めよう。

177 と 52 でユークリッドの互除法を使うと次のようになる。

$177\div52=3$あまり21

$52\div21=2$あまり10

$21\div10=2$あまり1

計算によって表すと次のようになる。

【計算３．１】

$$\begin{array}{r} 3 \\ 52\,\overline{)\,177} \\ 156 \\ \hline 21 \end{array} \qquad \begin{array}{r} 2 \\ 21\,\overline{)\,52} \\ 42 \\ \hline 10 \end{array} \qquad \begin{array}{r} 2 \\ 10\,\overline{)\,21} \\ 20 \\ \hline 1 \end{array}$$

ここから

$177\div52=3$あまり21　より $177=52\times3+21$　$\therefore\ 21=177-52\times3$　…①

$52\div21=2$あまり10　より $52=21\times2+10$　$\therefore\ 10=52-21\times2$　…②

$21\div10=2$あまり1　より $21=10\times2+1$　$\therefore\ 1=21-10\times2$　…③

③に②を代入して　$1=21-(52-21\times2)\times2$

$52\times(-2)+21\times5=1$

①を代入して　$52\times(-2)+(177-52\times3)\times5=1$

$52\times(-17)+177\times5=1$

つまり $177\times5-52\times17=1$ を満たすから整数 $(x,y)=(5,17)$

確かにこの方法で求めることができるが、計算が煩雑で生徒の理解を得るのが難しい。

そこで、次のように考えてみたい。

３．２　一次不定方程式の解の別解

３．１のユークリッドの互除法を行ったうえで、 $a=177$ 、 $b=52$ とおく。

【計算３．１】の商の部分（赤色の部分）をかえずにもう一度ユークリッドの互除法の計算を行う。

【計算３．２】

$$\begin{array}{r} 3 \\ b\,\overline{)\,a} \\ 3b \\ \hline a-3b \end{array} \qquad \begin{array}{r} 2 \\ a-3b\,\overline{)\,b} \\ 2a-6b \\ \hline -2a+7b \end{array} \qquad \begin{array}{r} 2 \\ -2a+7b\,\overline{)\,a-3b} \\ -4a+14b \\ \hline 5a-17b \end{array}$$

【計算３．１】と【計算３．２】は同じ計算を行っているから、それぞれの位置は対応している。

したがって、緑の部分の計算は等しいから

$5a-17b=1$ である。

$a=177$ 、 $b=52$ を元に戻して

$5\times177-17\times52=1$

つまり $177\times5-52\times17=1$ より $(x,y)=(5,17)$ である。

§４　まとめ

ユークリッドの互除法を教科書通りに理解するのは難しい。しかしながら、正方形の敷き詰めや分数を使って理解することで実は簡単なものなのではないかと思う。数学を単なる方法論の暗記にせずに、理解を伴った勉強にしたいなと思う。