拡張ユークリッド互除法について

担当：大矢 浩徳 (OYA Hironori)

本資料では，ユークリッド互除法および拡張ユークリッド互除法の厳密な取扱いを示しておく[*1]．

定義

正の整数 $a, b \in \mathbb{Z}_{>0}$ に対して，その最大公約数を $\gcd(a, b)$ と書く．さらに $a, b \in \mathbb{Z}$ に対する $\gcd(a, b)$ を以下のように定義する：

- 任意の 0 以上の整数 $a \in \mathbb{Z}_{\geq 0}$ に対して $\gcd(0, a) = \gcd(a, 0) = a$ とする．
- 各 $a, b \in \mathbb{Z}$ に対し，$\gcd(a, b) := \gcd(|a|, |b|)$ とする．

例 1.

$$\gcd(20, 8) = 4 \qquad \gcd(0, 7) = 7 \qquad \gcd(42, -54) = 6 \qquad \gcd(-5, 0) = 5.$$

注意 1.
- この定義は要するに「マイナスは無視して最大公約数を考えよ.」 ということである．
- 定義より，$\gcd(a, b) = 0$ となるのは，$(a, b) = (0, 0)$ のときのみであり，それ以外の時は $\gcd(a, b)$ は正の整数である．
- 各 $a, b \in \mathbb{Z}$ に対し，$\gcd(a, b) = \gcd(b, a)$ である．

補題

$a, b \in \mathbb{Z}$ が，ある $c \in \mathbb{Z}_{\geq 0}, d, d' \in \mathbb{Z}$ によって $a = cd, b = cd'$ と書けるとき，c を a と b の公約数ということにする．$(a, b) \neq (0, 0)$ のとき，$\gcd(a, b)$ は a と b の公約数の中で最大のものである．

補題の証明は容易なので省略する．ただし，この補題は $a \in \mathbb{Z}_{>0}$ に対し，$\gcd(0, a) = \gcd(a, 0) = a$ と定義しておかないと成立しないことに注意する．以下は gcd の重要な性質である．

命題

任意の $a, b, r \in \mathbb{Z}$ に対し，

$$\gcd(a, b) = \gcd(a + rb, b).$$

証明. $(a, b) = (0, 0)$ のとき主張は自明なので，$(a, b) \neq (0, 0)$ と仮定する．$\gcd(a, b) = c$, $\gcd(a + rb, b) = c'$ とし，$c = c'$ を証明すればよい．$a = cd_1$, $b = cd_1'$, $a + rb = c'd_2$, $b = c'd_2'$ とする $(d_1, d_1', d_2, d_2' \in \mathbb{Z})$．このとき，

$$a + rb = cd_1 + rcd_1' = c(d_1 + rd_1')$$

なので，$a + rb$ も b も c で割り切れることから，補題より，$c' = \gcd(a + rb, b) \geq c$ である．一方，

$$a = a + rb - rb = c'd_2 - rc'd_2' = c'(d_2 - rd_2')$$

なので，a も b も c' で割り切れることから，補題より，$c = \gcd(a, b) \geq c'$ である．以上より，$c = c'$ である．□

$a, b \in \mathbb{Z}$ に対して $\gcd(a, b)$ を求めたいときは，定義より $\gcd(|a|, |b|)$ を求めればよい．これより，$a \in \mathbb{Z}_{>0}$, $b \in \mathbb{Z}_{>0}$ の場合に $\gcd(a, b)$ を求める方法を知っていれば十分である (どちらかが 0 の場合は容易なので，それ以外の場合を考える)．この方法の一つがユークリッド互除法である．

[*1] 拡張ユークリッド互除法の解説について，大阪大学の有木進先生からいただいたコメントをもとに改良を加えました．有木進先生にこの場で御礼申し上げます．

ユークリッド互除法

$a, b \in \mathbb{Z}_{>0}, a \geq b$ とする．このとき，以下の操作を行う：

(0) $a_1 := a$, $b_1 := b$ とおいて，ステップ (1) へ進む.

(1) $a_1 = q_1 b_1 + r_1$ なる $q_1 \in \mathbb{Z}_{>0}$, $0 \leq r_1 < b_1$ を取る (q_1, r_1 はそれぞれ a_1 を b_1 で割った時の商と余り)．$r_1 = 0$ のときここで終了し，$r_1 \neq 0$ のとき，$a_2 := b_1$, $b_2 := r_1$ とおいて，ステップ (2) へ進む.

(2) $a_2 = q_2 b_2 + r_2$ なる $q_2 \in \mathbb{Z}_{>0}$, $0 \leq r_2 < b_2$ を取る (q_2, r_2 はそれぞれ a_2 を b_2 で割った時の商と余り)．$r_2 = 0$ のときここで終了し，$r_2 \neq 0$ のとき，$a_3 := b_2$, $b_3 := r_2$ とおいて，ステップ (3) へ進む.

$\cdots$

(k) $a_k = q_k b_k + r_k$ なる $q_k \in \mathbb{Z}_{>0}$, $0 \leq r_k < b_k$ を取る (q_k, r_k はそれぞれ a_k を b_k で割った時の商と余り)．$r_k = 0$ のときここで終了し，$r_k \neq 0$ のとき，$a_{k+1} := b_k$, $b_{k+1} := r_k$ とおいて，ステップ $(k+1)$ へ進む.

$\cdots$

このとき，この操作は必ずあるステップで終了し，ステップ (n) で終了したとき，$b_n = \gcd(a, b)$ である．

操作が有限回のステップで終了することの証明.

定義より，$b_1 > r_1 = b_2 > r_2 = b_3 > r_3 = b_4 > \cdots$ となるが，任意の ℓ に対し $r_\ell \geq 0$ となることから，この操作は有限回で止まる． □

ステップ (n) で終了したとき，$b_n = \gcd(a, b)$ であることの証明.

命題より，

$$\begin{aligned}\gcd(a, b) &= \gcd(a_1, b_1) = \gcd(a_1 - q_1 b_1, b_1) = \gcd(r_1, b_1) \\ &= \gcd(a_2, b_2) = \gcd(a_2 - q_2 b_2, b_2) = \gcd(r_2, b_2) \\ &= \gcd(a_3, b_3) = \cdots \\ &= \gcd(a_n, b_n) = \gcd(a_n - q_n b_n, b_n) = \gcd(r_n, b_n) = \gcd(0, b_n) = b_n\end{aligned}$$

である． □

代数学 I 第 3 解講義資料で述べたように，このユークリッド互除法の途中経過を記録していけば，その計算を逆にたどることで，

$$ax + by = \gcd(a, b) \tag{$*$}$$

を満たす整数の組 (x, y) を見つけることができる．しかし，ここでは「途中経過を記録しておいて逆にたどる」のではなく，ひと工夫を加えておくことで，「ユークリッドの互除法の終了とともに $(*)$ の整数解が見つかる」というような手法を紹介する．これが**拡張ユークリッド互除法**である．まず，ユークリッド互除法の過程

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} \rightsquigarrow \cdots \rightsquigarrow \begin{pmatrix} a_k \\ b_k \end{pmatrix} \rightsquigarrow \cdots$$

は以下のように行列を用いて表すことができる．

$$\begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} = \begin{pmatrix} b_1 \\ a_1 - q_1 b_1 \end{pmatrix} = \begin{pmatrix} b_1 \\ r_1 \end{pmatrix} = \begin{pmatrix} a_2 \\ b_2 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} = \begin{pmatrix} b_2 \\ a_2 - q_2 b_2 \end{pmatrix} = \begin{pmatrix} b_2 \\ r_2 \end{pmatrix} = \begin{pmatrix} a_3 \\ b_3 \end{pmatrix}$$

$$\cdots$$

$$\begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix} \begin{pmatrix} a_k \\ b_k \end{pmatrix} = \begin{pmatrix} b_k \\ a_k - q_k b_k \end{pmatrix} = \begin{pmatrix} b_k \\ r_k \end{pmatrix} = \begin{pmatrix} a_{k+1} \\ b_{k+1} \end{pmatrix}$$

$$\cdots$$

これより，ステップ (n) でユークリッド互除法が終了するとき，

$$\begin{pmatrix}\gcd(a,b)\\0\end{pmatrix}=\begin{pmatrix}b_n\\r_n\end{pmatrix}=\begin{pmatrix}0&1\\1&-q_n\end{pmatrix}\begin{pmatrix}a_n\\b_n\end{pmatrix}=\begin{pmatrix}0&1\\1&-q_n\end{pmatrix}\begin{pmatrix}0&1\\1&-q_{n-1}\end{pmatrix}\begin{pmatrix}a_{n-1}\\b_{n-1}\end{pmatrix}=\cdots$$
$$=\begin{pmatrix}0&1\\1&-q_n\end{pmatrix}\begin{pmatrix}0&1\\1&-q_{n-1}\end{pmatrix}\cdots\begin{pmatrix}0&1\\1&-q_1\end{pmatrix}\begin{pmatrix}a_1\\b_1\end{pmatrix}$$

ここで，

$$\begin{pmatrix}X&Y\\Z&W\end{pmatrix}:=\begin{pmatrix}0&1\\1&-q_n\end{pmatrix}\begin{pmatrix}0&1\\1&-q_{n-1}\end{pmatrix}\cdots\begin{pmatrix}0&1\\1&-q_1\end{pmatrix}$$

とすると，

$$\begin{pmatrix}\gcd(a,b)\\0\end{pmatrix}=\begin{pmatrix}X&Y\\Z&W\end{pmatrix}\begin{pmatrix}a_1\\b_1\end{pmatrix}=\begin{pmatrix}X&Y\\Z&W\end{pmatrix}\begin{pmatrix}a\\b\end{pmatrix}=\begin{pmatrix}aX+bY\\aZ+bW\end{pmatrix}.$$

なので，(X,Y) が $(*)$ を満たす整数の組 (x,y) の 1 つである．これより，行列 $\begin{pmatrix}X&Y\\Z&W\end{pmatrix}$ が求まれば $(*)$ を満たす整数の組 (x,y) が求まるが，定義より，これは $\begin{pmatrix}0&1\\1&-q_k\end{pmatrix}$ という形の行列を次々に左から掛けることで得られる．よって，以下のように $(*)$ の整数解 (x,y) を求められることがわかる．

拡張ユークリッド互除法

$a,b\in\mathbb{Z}_{>0}, a\geq b$ とする．このとき，以下の操作を行う：

(0) $a_1:=a$, $b_1:=b$ とおいて，ステップ (1) へ進む．

(1) $a_1=q_1b_1+r_1$ なる $q_1\in\mathbb{Z}_{>0}$, $0\leq r_1<b_1$ を取り (q_1, r_1 はそれぞれ a_1 を b_1 で割った時の商と余り)，行列

$$\begin{pmatrix}x_1&y_1\\z_1&w_1\end{pmatrix}:=\begin{pmatrix}0&1\\1&-q_1\end{pmatrix}$$

を考える．$r_1=0$ のときここで終了し，$r_1\neq0$ のとき，$a_2:=b_1$, $b_2:=r_1$ とおいて，ステップ (2) へ進む．

(2) $a_2=q_2b_2+r_2$ なる $q_2\in\mathbb{Z}_{>0}$, $0\leq r_2<b_2$ を取り (q_2, r_2 はそれぞれ a_2 を b_2 で割った時の商と余り)，行列

$$\begin{pmatrix}x_2&y_2\\z_2&w_2\end{pmatrix}:=\begin{pmatrix}0&1\\1&-q_2\end{pmatrix}\begin{pmatrix}x_1&y_1\\z_1&w_1\end{pmatrix}$$

を考える．$r_2=0$ のときここで終了し，$r_2\neq0$ のとき，$a_3:=b_2$, $b_3:=r_2$ とおいて，ステップ (3) へ進む．

$\cdots$

(k) $a_k=q_kb_k+r_k$ なる $q_k\in\mathbb{Z}_{>0}$, $0\leq r_k<b_k$ を取り (q_k, r_k はそれぞれ a_k を b_k で割った時の商と余り)，行列

$$\begin{pmatrix}x_k&y_k\\z_k&w_k\end{pmatrix}:=\begin{pmatrix}0&1\\1&-q_k\end{pmatrix}\begin{pmatrix}x_{k-1}&y_{k-1}\\z_{k-1}&w_{k-1}\end{pmatrix}$$

を考える．$r_k=0$ のときここで終了し，$r_k\neq0$ のとき，$a_{k+1}:=b_k$, $b_{k+1}:=r_k$ とおいて，ステップ $(k+1)$ へ進む．

$\cdots$

このとき，この操作は必ずあるステップで終了し，ステップ (n) で終了したとき，

$$b_n=\gcd(a,b),\qquad ax_n+by_n=\gcd(a,b)$$

である．

言葉で書けば拡張ユークリッド互除法とは，「ユークリッドの互除法を進めていく際に，ある行列をあわせて記録しておくことで，ユークリッドの互除法が終了した時点で $ax+by=\gcd(a,b)$ を満たす整数の組 (x,y) も

同時に得る」という手法である．とくに，拡張ユークリッド互除法を用いれば，$ax+by=\gcd(a,b)$ を満たす整数の組 (x,y) を求める際にもユークリッドの互除法の途中経過を覚えておく必要がないということに注意しよう．

例 2. $2394x+714y=\gcd(2394,714)$ を満たす整数の組 (x,y) を拡張ユークリッド互除法で 1 つ求めてみる．

(Step 1) $2394=\underset{\text{商}}{3}\times 714+\underset{\text{余り}}{252}$ なので，行列

$$\begin{pmatrix}0 & 1\\ 1 & -3\end{pmatrix}$$

を準備する．

(Step 2) $714=\underset{\text{商}}{2}\times 252+\underset{\text{余り}}{210}$ なので，Step1 で準備した行列に左から $\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}$ を掛けて，

$$\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -3\end{pmatrix}=\begin{pmatrix}1 & -3\\ -2 & 7\end{pmatrix}$$

を得る．

(Step 3) $252=\underset{\text{商}}{1}\times 210+\underset{\text{余り}}{42}$ なので，Step2 で得られた行列に左から $\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}$ を掛けて，

$$\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1 & -3\\ -2 & 7\end{pmatrix}=\begin{pmatrix}-2 & 7\\ 3 & -10\end{pmatrix}$$

を得る．

(Step 4) $210=\underset{\text{商}}{5}\times 42+\underset{\text{余り}}{0}$ なので，Step3 で得られた行列に左から $\begin{pmatrix}0 & 1\\ 1 & -5\end{pmatrix}$ を掛けて，

$$\begin{pmatrix}0 & 1\\ 1 & -5\end{pmatrix}\begin{pmatrix}-2 & 7\\ 3 & -10\end{pmatrix}=\begin{pmatrix}3 & -10\\ -17 & 57\end{pmatrix}$$

を得る．ここで余りが 0 となったのでストップする．

このとき，$\gcd(2394,714)=42$ であることがわかり，最終的に得られた行列の 1 行目の $(3,-10)$ が $2394x+714y=42$ を満たす整数の組 (x,y) の 1 つとなっている．

コラム：連分数との関係

次のような分母にさらに分数が含まれているような数の表記を (単純) **連分数**という：

$$q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\cfrac{1}{\ddots+\cfrac{1}{q_n}}}}$$

ただし，$q_1\in\mathbb{Z},q_2,\dots,q_n\in\mathbb{Z}_{>0}$．有理数が与えられたとき，その連分数展開はユークリッド互除法を用いて次のように求めることができる．

2 ページ目上部のユークリッド互除法の説明中に用いられた記号を用いて $a,b\in\mathbb{Z}_{>0},a\geq b$ に対して，a/b の連分数展開を求める．ここでユークリッド互除法はステップ n で終わるとする (つまり $r_n=0$)．いま

$a = a_1, b = b_1, a_1 = q_1 b_1 + r_1$ より，

$$\begin{aligned}
\frac{a}{b} &= \frac{a_1}{b_1} = q_1 + \frac{r_1}{b_1} = q_1 + \frac{1}{\frac{b_1}{r_1}} = q_1 + \frac{1}{\frac{a_2}{b_2}} \\
&= q_1 + \frac{1}{q_2 + \frac{r_2}{b_2}} = q_1 + \frac{1}{q_2 + \frac{1}{\frac{b_2}{r_2}}} = q_1 + \frac{1}{q_2 + \frac{1}{\frac{a_3}{b_3}}} \\
&= \cdots \\
&= q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots + \cfrac{1}{q_{n-1} + \cfrac{r_{n-1}}{b_{n-1}}}}}} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{\frac{b_{n-1}}{r_{n-1}}}}}}} \\
&= q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{\frac{a_n}{b_n}}}}}} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}
\end{aligned}$$

ちなみに，$a \leq b$ の場合には，$\dfrac{a}{b} = \dfrac{1}{\frac{b}{a}}$ より，$q_1 = 0$ であると考えて先に進めば，以降は同じである．また，$a < 0, b > 0$ のときも，

$$a = q_1 b + r_1,\ q_1 \in \mathbb{Z}_{<0}, 0 \leq r_1 < b$$

を満たす q_1, r_1 をとることができ，このとき $\dfrac{a}{b} = q_1 + \dfrac{r_1}{b}$ となるので，q_1 が負の値をとるだけで以降は同じである．

上でユークリッド互除法のアルゴリズムは必ず終了することを見たので，以下がわかる：

定理

任意の有理数は (有限の長さで) 連分数展開できる．

例 3. $\dfrac{2394}{714}$ の連分数展開を求めてみる：

$$\begin{aligned}
2394 &= 3 \times 714 + 252 & 714 &= 2 \times 252 + 210 \\
252 &= 1 \times 210 + 42 & 210 &= 5 \times 42 + 0
\end{aligned}$$

であったので，

$$\begin{aligned}
\frac{2394}{714} &= 3 + \frac{252}{714} = 3 + \frac{1}{\frac{714}{252}} \\
&= 3 + \frac{1}{2 + \frac{210}{252}} = 3 + \frac{1}{2 + \frac{1}{\frac{252}{210}}} \\
&= 3 + \frac{1}{2 + \frac{1}{1 + \frac{42}{210}}} = 3 + \frac{1}{2 + \frac{1}{1 + \frac{1}{\frac{210}{42}}}} = 3 + \frac{1}{2 + \frac{1}{1 + \frac{1}{5}}}
\end{aligned}$$