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，拡張ユークリッド互除法の “厳密な” 取扱いを示しておく．

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[*1]．
- 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 $c, d, d' \in \mathbb{Z}$ 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)．この方法の一つにユークリッド互除法がある．

[*1] 講義中には $\gcd(0, a) = \gcd(a, 0) = 0$ と書いてたが，$\gcd(0, a) = \gcd(a, 0) = a$ の方が良いので定義を修正する．

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. □

このユークリッド互除法の途中経過を用いて，$ax + by = \gcd(a, b)$ を満たす整数の組 (x, y) を見つけることができる．これを**拡張ユークリッド互除法**という．ユークリッド互除法の途中経過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，

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

ここで，

$$\begin{pmatrix} x_0 & y_0 \\ z_0 & w_0 \end{pmatrix} := \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{n-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix}$$

とすると，

$$\begin{pmatrix} \gcd(a,b) \\ 0 \end{pmatrix} = \begin{pmatrix} x_0 & y_0 \\ z_0 & w_0 \end{pmatrix} \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} = \begin{pmatrix} x_0 & y_0 \\ z_0 & w_0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} ax_0 + by_0 \\ az_0 + bw_0 \end{pmatrix}.$$

なので，(x_0, y_0) が $ax + by = \gcd(a, b)$ を満たす整数の組 (x, y) の 1 つである．

例 2. $2394x + 714y = \gcd(2394, 714)$ を満たす整数の組 (x, y) を 1 つ求めてみる．ここでは，講義で扱った方法とこの資料で説明した方法を比較しておく．まず，$\gcd(2394, 714)$ を求める：

$$2394 = 3 \times 714 + 252 \qquad 714 = 2 \times 252 + 210$$
$$252 = 1 \times 210 + 42 \qquad 210 = 5 \times 42 + 0$$

であるので，$\gcd(2394, 714) = \gcd(714, 252) = \gcd(252, 210) = \gcd(210, 42) = \gcd(42, 0) = 42$.

【講義で行った方法】

$$\begin{aligned} 42 &= 1 \times 252 + (-1) \times 210 \\ &= 1 \times 252 + (-1) \times (714 - 2 \times 252) = (-1) \times 714 + 3 \times 252 \\ &= (-1) \times 714 + 3 \times (2394 - 3 \times 714) = 3 \times 2394 + (-10) \times 714. \end{aligned}$$

より，$(x, y) = (3, -10)$ が $2394x + 714y = \gcd(2394, 714)$ を満たす整数の組 (x, y) の例である．

【この資料で行った方法】

$$\begin{aligned} \begin{pmatrix} x_0 & y_0 \\ z_0 & w_0 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & -5 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \\ &= \begin{pmatrix} 1 & -1 \\ -5 & 6 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \\ &= \begin{pmatrix} -1 & 3 \\ 6 & -17 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \\ &= \begin{pmatrix} 3 & -10 \\ -17 & 57 \end{pmatrix} \end{aligned}$$

となるので，$(x_0, y_0) = (3, -10)$ が $2394x + 714y = \gcd(2394, 714)$ を満たす整数の組 (x, y) の例である．ここで，行列の積は左のものから順に計算している．

これらを見比べると，色を付けた部分の数がそれぞれ対応していることがわかる．実際にこれらは一般的に一致することがわかり (確かめてみよ)，この資料での計算と講義で紹介した計算は同じ計算手続きとなる．