拡張ユークリッド法*

2019/7/3/14:44

1 本稿の目的

本稿の目的は、拡張ユークリッド法について説明することである。一般に、2つの正整数 a, b とその最大公約数 $\gcd(a, b)$ に対し、以下のような関係を満たす整数 f, g が存在する。

$$fa + gb = \gcd(a, b) \quad (1)$$

このとき、互助法ともよばれるユークリッド法は、与えられた正整数 a, b に対し、その最大公約数 $\gcd(a, b)$ を求める方法とすると、拡張ユークリッド法は、式(1)を満たす整数 f, g と $\gcd(a, b)$ を求める方法となる。

2 ユークリッド法のキーポイント

2.1 $\gcd(a, b) = \gcd(b, r_1)$ の成立

$a \geq b$ を満たす正の整数 a, b に対し、 a を b で割った商を q_1 , 余りを r_1 とすると

$$a = q_1b + r_1, \quad 0 \leq r_1 < b \quad (2)$$

と表すことができる。

はじめに、 $\gcd(a, b) = \gcd(b, r_1)$ となることを示す。 a と b の公約数を m とすると、 $r_1 = a - q_1b$ より、 r_1 は m を約数としてもつ。したがって、 $\gcd(a, b) \leq \gcd(b, r_1)$ が成り立つ。一方、 b と r_1 の公約数を m とすると、 $a = q_1b + r_1$ より、 a は m を約数としてもつ。したがって、 $\gcd(b, r_1) \leq \gcd(a, b)$ が成り立つ。ゆえに、 $\gcd(a, b) = \gcd(b, r_1)$ となる。

次に、 $r_{-1} = a, r_0 = b$ として、添字 $i = 1, 2, \dots, n, n+1$ に対し、 r_{i-2} を r_{i-1} で割ったときの商を q_i , 余りを r_i とすることで、以下のように書くことができる。ただし、 $0 \leq r_i < r_{i-1}$ である。なぜならば、 r_i は単調に減少していくので、 $r_{-1} > r_0 > \dots > r_n > r_{n+1} = 0$ となる。

$$r_{-1} = q_1r_0 + r_1 \quad (3)$$

$$r_0 = q_2r_1 + r_2 \quad (4)$$

$$\vdots \quad \vdots$$

$$r_{i-2} = q_i r_{i-1} + r_i \quad (5)$$

$$\vdots \quad \vdots$$

$$r_{n-2} = q_n r_{n-1} + r_n \quad (6)$$

$$r_{n-1} = q_{n+1} r_n \quad (7)$$

このとき、前述にて示したことより、以下のことが成り立つことに注意する:

$$\begin{aligned} \gcd(a, b) &= \gcd(r_{-1}, r_0) \\ &= \gcd(r_0, r_1) \\ &\quad \vdots \\ &= \gcd(r_{n-1}, r_n) = r_n \end{aligned}$$

2.2 $f_n a + g_n b = \gcd(a, b) = r_n$ の成立

次に、整数 f_i, g_i を

$$f_i a + g_i b = r_i \quad (8)$$

を満たすものとする。そして、

$$f_{-1} = 1, \quad g_{-1} = 0 \quad (9)$$

*栗原正純, 電気通信大学 (2019/7/3/14:44)

$$f_0 = 0, \quad g_0 = 1 \quad (10)$$

とすると、 $i = -1, 0$ において、式 (8) は成立する。そこで、式 (8) は $i = -1, 0, 1, \dots, k-1$ において成立すると仮定する。

今、 f_k, g_k を

$$f_k = f_{k-2} - q_k f_{k-1} \quad (11)$$

$$g_k = g_{k-2} - q_k g_{k-1} \quad (12)$$

として、式 (8) の $i = k$ の場合である

$$f_k a + g_k b = r_k \quad (13)$$

が成り立つことを示そう。式 (13) の左辺に式 (11) と (12) を代入し、整理すると、仮定より、以下が成り立つ。

$$\begin{aligned} f_k a + g_k b &= (f_{k-2} - q_k f_{k-1})a + (g_{k-2} - q_k g_{k-1})b \\ &= (f_{k-2}a + g_{k-2}b) - q_k(f_{k-1}a + g_{k-1}b) \\ &= r_{k-2} - q_k r_{k-1} = r_k \end{aligned}$$

上記最後の等号は、式 (5) の $i = k$ の場合による。以上より、数学的帰納法より、任意の $i = -1, 0, 1, \dots, n$ に対し、式 (13) は成り立つ。

ゆえに、 a と b の最大公約数 $\gcd(a, b) = r_n$ は f_n と g_n を用いて以下のように表すことができる：

$$f_n a + g_n b = r_n$$

3 拡張ユークリッド法

改めて、与えられた整数 a, b に対する拡張ユークリッド法の手続きを記す。ただし、 $a > b$ とする。

3.1 拡張ユークリッド法の手続き

1. (初期設定) まず、添字 $i := 1$ とする。

$$r_{-1} := a, \quad f_{-1} := 1, \quad g_{-1} = 0$$

$$r_0 := b, \quad f_0 := 0, \quad g_0 = 1$$

2. (q_i, r_i の更新) r_{i-2}, r_{i-1} から以下を満たす q_i, r_i を求める：

$$r_{i-2} = q_i r_{i-1} + r_i, \quad 0 \leq r_i < r_{i-1}$$

3. (f_i, g_i の更新) 上記で求めた q_i を用いて以下を計算する：

$$f_i = f_{i-2} - q_i f_{i-1} \quad (14)$$

$$g_i = g_{i-2} - q_i g_{i-1} \quad (15)$$

4. (終了条件のチェック) $r_i = 0$ ならば、式 (1) を満たす値を以下のように設定し、手続きを終了する：

$$\gcd(a, b) := r_{i-1} \quad (16)$$

$$f := f_{i-1} \quad (17)$$

$$g := g_{i-1} \quad (18)$$

他方、 $r_i \neq 0$ ならば、 $i := i + 1$ として、手続き 2 へ戻る。

3.2 例

$(a, b) = (144, 60)$ の場合の例を示す：

i	f_i	g_i	r_i	q_i
-1	1	0	144	-
0	0	2	60	-
1	1	-2	24	2
2	-2	5	12	2
3	5	-12	0	2

(19)

上記結果より、 $\gcd(144, 60) = 12$ で、以下が成り立つ：

$$-2 \times 144 + 5 \times 60 = 12 \quad (20)$$