ユークリッドの互除法

1. 記法について

以下では、自然数の集合$\{1, 2, 3, \ldots\}$を$\mathcal{N}$で表し、整数の集合$\{0, \pm1, \pm2, \pm3, \ldots\}$を$\mathcal{Z}$で表す。整数$a \neq 0$および$b$について、$b$が$a$で割り切れるとき、$a|b$と表記する。逆に割り切れないときは、$a \not| b$と表す。$a|b$であるとき、$a$は$b$の**約数**であるといい、$b$は$a$の**倍数**であるという。$d|a$かつ$d|b$であるとき、$d$は$a$と$b$の**公約数**であるというが、公約数のうち最大のものを**最大公約数**と呼ぶ。aとbの最大公約数を(a, b)と表記する。aとbの最大公約数が1、すなわち$(a, b) = 1$であるとき、aとbは**互いに素**であるという。

2. 除法定理

整数a、$b > 0$があるとき、aをbで割って、商qと余りr（$0 \leq r < b$）を**一意に**求めることができる。このとき、

$$a = bq + r \qquad (1)$$

が成立する。

3. ユークリッドの互除法

3.1 原理

正の整数aとb（$a > b$とする）の最大公約数$d = (a, b)$を求める方法を考える。もし、$b|a$ならば、明らかに$d = b$である。$b \not| a$のときは、式(1)によって、余り$r > 0$を求めることができる。このとき、

$$d = (a, b) = (b, r) \qquad (2)$$

が成り立つ。なぜなら、$d = (a, b)$より、$a = da'$、$b = db'$（$(a', b') = 1$）とおけるので、式(1)より、

$$r = d(a' - b'q)$$

となり、rはdを約数に持つ。ここで、もし、$d' = (b, r) > d$であるとすると、上と同様にして、d'はaの約数でもあることになり、$d = (a, b)$に矛盾する。従って、$d' = d$であり、式(2)が成立することがわかる。

式(2)において、$a > b$、$b > r$であるから、aとbの最大公約数dを求めるかわりに、より小さい数であるbとrの最大公約数を求めてもよいことがわかる。この関係を繰り返し利用して、最大公約数を求めるアルゴリズムがユークリッドの互除法である。すなわち、上記のbをrでさらに割って余りr_1を求める。この作業を以下のように繰り返し行なうと、余りは単調に減少していくので有限回の演算の後に余りが0になるはずである。

$$\begin{aligned} a &= bq + r \\ b &= rq_1 + r_1 \\ r &= r_1 q_2 + r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + r_n \\ r_{n-1} &= r_n q_{n+1} \end{aligned} \qquad (3)$$

上式より、

$$(a, b) = (b, r) = (r, r_1) = \cdots = (r_{n-1}, r_n) = r_n = d$$

となることがわかる。

3.2 具体例

具体例として、$(1785, 1122)$を求めてみよう。ユークリッドの互除法を実行すると以下のようになる。

$$\begin{aligned} 1785 &= 1122 \times 1 + 663 \\ 1122 &= 663 \times 1 + 459 \\ 663 &= 459 \times 1 + 204 \end{aligned}$$

$$
\begin{aligned}
459 &= 204 \times 2 + 51 \\
204 &= 51 \times 4
\end{aligned}
$$

これより、$(1785, 1122) = 51$ と求まる。

4. 拡張ユークリッドの互除法

正の整数 a、b の最大公約数 $d = (a, b)$ であるとき、

$$d = sa + tb \tag{4}$$

を満たす整数 s、t が存在する。これは、式 (3) の最後から 2 番目の式を

$$d = r_n = r_{n-2} - r_{n-1}q_n$$

と変形し、式 (3) の各式を逆にたどっていくことで容易に示すことができる。3.2 の例を用いてこのことを確かめてみよう。

$$
\begin{aligned}
51 &= 459 - 204 \times 2 \\
&= 459 - (663 - 459 \times 1) \times 2 \\
&= -2 \times 663 + 3 \times 459 \\
&= -2 \times 663 + 3 \times (1122 - 663 \times 1) \\
&= 3 \times 1122 - 5 \times 663 \\
&= 3 \times 1122 - 5 \times (1785 - 1122 \times 1) \\
&= -5 \times 1785 + 8 \times 1122
\end{aligned}
$$

上記より、$s = -5$、$t = 8$ であることがわかる。

次に、式 (3) を逆にたどることなく、逐次的に s、t を求める方法を考えてみる。

まず、

$$r_i = s_i a + t_i b \tag{5}$$

とおく。すると、

$$
\begin{aligned}
r_i &= r_{i-2} - r_{i-1}q_i \\
&= (s_{i-2}a + t_{i-2}b) - q_i(s_{i-1}a + t_{i-1}b) \\
&= (s_{i-2} - q_i s_{i-1})a + (t_{i-2} - q_i t_{i-1})b
\end{aligned}
$$

であるから、s_i、t_i に関する漸化式

$$
\begin{aligned}
s_i &= s_{i-2} - q_i s_{i-1} \\
t_i &= t_{i-2} - q_i t_{i-1}
\end{aligned}
$$

表 1: 拡張ユークリッドの互除法の例

i	q_i	r_i	s_i	t_i
0	1	663	1	-1
1	1	459	-1	2
2	1	204	2	-3
3	2	51	-5	8
4	4	0	-	-

を得る。なお、s_i、t_i の初期値は、$r_0 = a - bq$ として係数を比較することにより、$s_{-2} = 1, s_{-1} = 0$ および、$t_{-2} = 0, t_{-1} = 1$ とすればよい。この漸化式を用いて、a と b から、最大公約数 d および s と t を求めるアルゴリズムを拡張ユークリッドの互除法と呼んでいる。3.2 の例に対して、拡張ユークリッドの互除法を実行する際の各ステップを表 1 に示す。各ステップにおいて、式 (5) の関係が成立しており、従って、$r_n = 0$ となった時に、$d = r_{n-1} = s_{n-1}a + t_{n-1}b$ であることがわかる。

5. $\mathcal{Z}_q$ における逆元の計算

整数 q を法とする合同式

$$ax \equiv 1 \bmod q \tag{6}$$

において、$(a, q) = 1$ ならば、解 $x (0 < x < q)$ が存在する。q を法とする剰余類環 $\mathcal{Z}_q$ を考えるとき、この元 x を元 a の逆元と呼び、a^{-1} と書く。拡張ユークリッドの互除法を用いると、この逆元を容易に求めることができる。

a と q の最大公約数は 1 であるので、拡張ユークリッドの互除法により

$$sa + tq = 1 \tag{7}$$

となる整数 s、t を求めることができる。この式より、$sa - 1 = -tq$ であるので、s は式 (6) を満たすことがわかる。拡張ユークリッドの互除法の結果が $s < 0$ となった場合には、$s \leftarrow s + q$ とすればよい。なお、逆元の計算では、t の値は不要であるので、アルゴリズム中の t に関する演算は省略できる。