アルゴリズム B 第 10 回　　2019 年 12 月 16 日

10　ユークリッドの互除法

ユークリッドの互除法

a, b を整数として，$a \neq 0$ とする．a が b を割り切るとき，$a \mid b$ と表す．

a, b を整数とする．a と b に共通な正の約数の中で最大のものを a と b の**最大公約数** (greatest common divisor) といい，$\gcd(a, b)$ で表す．ただし，$a = b = 0$ のときは $\gcd(0, 0) = 0$ と定める．特に，任意の整数 a に対して，$\gcd(a, 0) = \gcd(0, a) = |a|$ である．$\gcd(a, b) = 1$ であるとき，a と b は**互いに素** (relatively prime) であるという．

第 1 回講義で紹介したように，最大公約数は**ユークリッドの互除法** (Euclidean algorithm) で計算できる．

ユークリッドの互除法を拡張することで 1 次不定方程式の解が計算できる．

定理 10.1. a, b を整数として，$d = \gcd(a, b)$ とおく．このとき，変数 X と Y に関する方程式

$$aX + bY = d \tag{1}$$

は整数解を持つ．

方程式 (1) の整数解は以下の方法で求められる．一般性を失うことなく $a \geq b > 0$ と仮定できる．

$$r_{-1} = a, \quad r_0 = b, \quad x_{-1} = 1, \quad x_0 = 0, \quad y_{-1} = 0, \quad y_0 = 1$$

とおく．$j = 1, 2, \ldots$ に対して，$r_{j-1} \neq 0$ ならば，

$$r_{j-2} = q_j r_{j-1} + r_j \quad (0 \leq r_j < r_{j-1}), \quad x_j = x_{j-2} - q_j x_{j-1}, \quad y_j = y_{j-2} - q_j y_{j-1}$$

によって整数 q_j, r_j, x_j, y_j を定める．このとき，$ax_j + by_j = r_j$ が成り立つ．特に，n を除算回数とすれば，$r_n = 0$ であり，$ax_{n-1} + by_{n-1} = r_{n-1} = d$ が成り立つ．このアルゴリズムを**拡張ユークリッドの互除法** (extended Euclidean algorithm) という．擬似コードでは次のように書ける．ただし，上の記号で (d, x_{n-1}, y_{n-1}) を返す．

```
ExtendedGCD(a, b)
  (s, r, u, x, v, y) = (a, b, 1, 0, 0, 1)
  while r ≠ 0
    q = ⌊s/r⌋
    (s, r, u, x, v, y) = (r, s − qr, x, u − qx, y, v − qy)
  return (s, u, v)
```

（拡張）ユークリッドの互除法の計算量について，乗除算を筆算と同様に行うと，次の定理が成り立つ．

定理 10.2. $\phi = (1 + \sqrt{5})/2$ とおく．任意の $a \geq b > 0$ に対して，（拡張）ユークリッドの互除法における除算回数は $\log_\phi(3 - \phi)(b + 1)$ 以下であり，ビット演算量は $O((\log a)(\log^2 b)) = O(\log^3 a)$ である．

注意. 計算量を精密に評価することで，ビット演算量が $O((\log a)(\log b)) = O(\log^2 a)$ であることもわかる．また，より高速な乗除算アルゴリズムを用いた場合は，（拡張）ユークリッドの互除法の計算量も減少する．

合同式

a, b を整数，n を自然数とする．$a-b$ が n で割り切れるとき，a と b は **n を法として合同である** (congruent modulo n) といい，$a \equiv b \pmod{n}$ と表す．このように $\equiv$ で結ばれた式を**合同式** (congruence) という．

関係 $\equiv \pmod{n}$ は $\mathbb{Z}$ 上の同値関係である．この同値関係による $\mathbb{Z}$ の商集合を $\mathbb{Z}/n\mathbb{Z}$ で表し，$a \in \mathbb{Z}$ が属する同値類を $a + n\mathbb{Z}$ で表す．すなわち，$\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\}$ である．

命題 10.3. a, b, c, d を整数，n を自然数とする．$a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$ のとき，次が成り立つ．

(a) $a + c \equiv b + d \pmod{n}$.
(b) $a - c \equiv b - d \pmod{n}$.
(c) $ac \equiv bd \pmod{n}$.

注意. 命題 10.3 より，$\mathbb{Z}/n\mathbb{Z}$ は自然に可換環となる．

定理 10.4. a, b を整数，n を自然数とする．a と n が互いに素なとき，1 次合同式

$$aX \equiv b \pmod{n} \tag{2}$$

は n を法としてただ 1 つ解を持つ．$0 < a < n$, $0 \le b < n$ のとき，解を求めるのに必要なビット演算量は $O(\log^3 n)$ である．

1 次合同式 (2) の解は次のように計算できる．拡張ユークリッドの互除法により $ax + ny = 1$ を満たす整数 x, y を計算する．このとき，$a(bx) + n(by) = b$ だから，$a(bx) \equiv b \pmod{n}$ となる．すなわち，$X = bx$ は (2) の解である．

定理 10.5 (**中国剰余定理** (Chinese remainder theorem))**.** $m_1, m_2, \ldots, m_r$ をどの 2 つも互いに素な自然数とする．$M = m_1 m_2 \cdots m_r$ とおく．任意の整数 $a_1, a_2, \ldots, a_r$ に対して，連立合同式

$$\begin{cases} X \equiv a_1 \pmod{m_1}, \\ X \equiv a_2 \pmod{m_2}, \\ \quad \cdots \\ X \equiv a_r \pmod{m_r} \end{cases} \tag{3}$$

は M を法としてただ 1 つ解を持つ．

連立合同式 (3) の解は次のように計算できる．$M_i = M/m_i$ とおいて，$M_i N_i \equiv 1 \pmod{m_i}$ を満たす整数 N_i を求める．このとき，$x = \sum_{i=1}^{r} a_i M_i N_i$ とおくと，$X = x$ は (3) の解である．

注意. 定理 10.5 の仮定の下で，写像

$$\begin{aligned} \mathbb{Z}/M\mathbb{Z} &\to \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}; \\ a + M\mathbb{Z} &\mapsto (a + m_1\mathbb{Z}, a + m_2\mathbb{Z}, \ldots, a + m_r\mathbb{Z}) \end{aligned}$$

は well-defined であり，環同型である．これも中国剰余定理と呼ばれる．