数学展望 I 第 7 回：ユークリッドの互除法

2 つの整数の最大公約数を求めるアルゴリズムとして, ユークリッドの互除法について述べる. また, 中国式剰余定理の利用方法も述べる.

6.1 ユークリッドの互除法

問 1. 次の問に答えよ.

(1) 140 と 58 の最大公約数 $(140, 58)$ を求めよ.

(2) $29m + 12n = 1$ を満たす整数の組 (m, n) をすべて決定せよ.

(注) (2) においては**まず 1 組見つけることが大事**である！

定理 6.1 (ユークリッドの互除法). a, b を正の整数とし, a を b で割った商を q, 余りを r とするとき, $a = qb + r$, $0 \leq r < b$ と書ける. a と b の最大公約数を (a, b) と表すとき,

$$(a, b) = (b, r)$$

が成立する. また, このような操作を高々 b 回行えば, 最大公約数が求まる.

(1)

$$\begin{aligned} \underline{140} &= 2 \times \underline{58} + \underline{24} \\ \underline{58} &= 2 \times \underline{24} + \underline{10} \\ \underline{24} &= 2 \times \underline{10} + \underline{4} \\ \underline{10} &= 2 \times \underline{4} + \underline{2} \\ \underline{4} &= 2 \times \underline{2} \end{aligned}$$

よって, $(140, 58) = (58, 24) = (24, 10) = (10, 4) = (4, 2) = 2$.

(2)

$$\begin{aligned} \underline{29} &= 2 \times \underline{12} + \underline{5} \cdots (1) \\ \underline{12} &= 2 \times \underline{5} + \underline{2} \cdots (2) \\ \underline{5} &= 2 \times \underline{2} + \underline{1} \cdots (3) \end{aligned}$$

を用いて,

$$\begin{aligned} 1 &= \underline{5} - 2 \times \underline{2} && (\because (3)) \\ &= \underline{5} - 2 \times (\underline{12} - 2 \times \underline{5}) && (\because (2)) \\ &= (-2) \times \underline{12} + 5 \times \underline{5} \\ &= (-2) \times \underline{12} + 5 \times (\underline{29} - 2 \times \underline{12}) && (\because (1)) \\ &= 5 \times \underline{29} + (-12) \times \underline{12} \end{aligned}$$

とすればよい. また, 一般解は次で与えられる:

$$m = \underline{12}k + 5, \quad n = -\underline{29}k - 12 \quad (k \text{ は整数}).$$

注意 1. a, b の**素因数分解**が求まるならば, その最大公約数を求めるのは容易である. しかしながら, 大きな数 (例えば, p, q が十分大きい素数のときの $n = pq$) の素因数分解を見い出すのは**計算機でも困難である**. 下の例題で実感せよ.

定理 6.2. 整数 $a_1, \ldots, a_n$ の最大公約数が d のとき,

$$a_1 m_1 + \cdots + a_n m_n = k$$

を満たす整数 $m_1, \ldots, m_n$ が存在するのは, k が d の倍数のときに限る.

系 6.3. a と b が**互いに素** $\iff$ $am + bn = 1$ をみたす整数 m, n が存在する.

例 6.4. ユークリッドの互除法を用いて, $a = 4189$ と $b = 3953$ の最大公約数を求めよ.

6.2 中国式剰余定理

問 2. 3 で割ると 2 余り, 4 で割ると 1 余り, 5 で割ると 3 余るような正の整数のうち, 最小のものを求めよ.

一般に次の定理が成り立つ. ただし, $N \equiv c \pmod{a}$ は $N - c$ が a で割り切れることを意味する.

定理 6.5 (中国式剰余定理). $a_1, \ldots, a_r$ を 互いに素 な正の整数とする. このとき, 任意の整数 $c_1, \ldots, c_r$ に対して,

$$N \equiv c_1 \pmod{a_1}, \quad N \equiv c_2 \pmod{a_2}, \quad \cdots, \quad N \equiv c_r \pmod{a_r}$$

を満たす整数 N が存在する. そのようなものの 1 つを N_0 とするとき,

$$N = a_1 a_2 \cdots a_r k + N_0 \quad (k \text{ は整数})$$

と書くことができる.

$r = 3$ の場合に, 定理の条件を満たす N を見つけるには,

$$\begin{array}{lll} n_1 \equiv 1 \pmod{a_1} & n_2 \equiv 0 \pmod{a_1} & n_3 \equiv 0 \pmod{a_1} \\ n_1 \equiv 0 \pmod{a_2} & n_2 \equiv 1 \pmod{a_2} & n_3 \equiv 0 \pmod{a_2} \\ n_1 \equiv 0 \pmod{a_3} & n_2 \equiv 0 \pmod{a_3} & n_3 \equiv 1 \pmod{a_3} \end{array}$$

となる n_1, n_2, n_3 を見つけて, $N_0 = c_1 n_1 + c_2 n_2 + c_3 n_3$ とすればよい.

n_1 **の見つけ方:** $(a_1, a_2 a_3) = 1$ に注意して, $a_1 m + a_2 a_3 n = 1$ となる整数 (m, n) を見つけて (**系 6.3 参照**), $n_1 = a_2 a_3 n (= 1 - a_1 m)$ とおけばよい.