§2. ユークリッドの互除法

与えられた整数 a, b の最大公約数を求める 1 つの方法は、a, b を素因数分解して、共通因数を取り出すことである。しかし、大きな整数を素因数分解することは難しい。このようなとき、ユークリッドの互除法が有効である。ユークリッドの互除法は、いかなる数に対しても、単純な手続きを経て最大公約数を求める方法を与える。この節では、まず、ユークリッドの互除法による最大公約数の求め方を説明し、次に、素因数分解による最大公約数の求め方を説明する。

● 2 - 1 : ユークリッドの互除法

ユークリッドの互除法は最大公約数を求めるための強力なアルゴリズムである。ユークリッドの互除法の基礎にあたるのが次の命題である。

命題 2 - 1 - 1
0 でない 2 つの整数 a, b $(b > 0)$ を、ある $q, r \in \mathbb{Z}$ を用いて $a = qb + r \ \ (0 \leq r < b)$ と書く。このとき、$\gcd(a, b) = \gcd(b, r)$ が成り立つ。

(**証明**)

$d = \gcd(a, b),\ d_1 = \gcd(b, r)$ とおく。$d|a$ と $d|b$ より $d|(a - qb)$, すなわち、$d|r$ を得る。よって、$d|d_1$ である (演習 1 - 1)。他方、$d_1|b$ と $d_1|r$ より $d_1|(qb + r)$, すなわち、$d_1|a$ を得る。よって、$d_1|d$ である。$d|d_1$ と $d_1|d$ から $d = \pm d_1$ になるが、$d, d_1 > 0$ だから $d = d_1$ を得る。 □

[命題 2 - 1 - 1] を $a \geq b$ の場合に適用することにより、a と b の最大公約数を求める問題がより小さい整数 b と r の最大公約数を求める問題に帰着されることがわかる。したがって、[命題 2 - 1 - 1] を繰り返し適用していけば最後には割り切れる状態になり、最大公約数が求まる。このようにして最大公約数を求める方法を**ユークリッドの互除法**という。

● 2 - 2 : 不定方程式

ユークリッドの互除法により a, b の最大公約数 d ばかりでなく、$ax + by = d$ を満たす $x, y \in \mathbb{Z}$ も求めることができる。

例 2 - 2 - 1 $d := \gcd(123, 33)$ を求め、$123x + 33y = d$ を満たす整数 x, y を 1 組求めよ。

解 ;

$$
\begin{aligned}
123 &= 3 \cdot 33 + 24, \\
33 &= 1 \cdot 24 + 9, \\
24 &= 2 \cdot 9 + 6, \\
9 &= 1 \cdot 6 + 3, \\
6 &= 2 \cdot 3
\end{aligned}
$$

左の計算結果から、$d = \gcd(6, 3) = 3$ とわかる。また、左の計算過程の最後から 2 番目の式より順次上に遡っていくことにより

$$3 = 9 - 1 \cdot 6 = 9 - 1 \cdot (24 - 2 \cdot 9) = \cdots = -4 \cdot 123 + 15 \cdot 33$$

を得る。こうして、$123x + 33y = 3$ を満たす整数の 1 組 $(x, y) = (-4, 15)$ が見つかる。 □

演習 2 - 1 * $d := \gcd(15640, 1037)$ を求め、$15640x + 1037y = d$ を満たす整数 x, y を 1 組求めよ。

一般に、0 でない 2 つの整数 a, b および整数 k に対して、$aX + bY = k$ という形の X, Y についての方程式を**不定方程式** (indeterminate equation) という。k が $d = \gcd(a, b)$ の倍数のとき、[系 1 - 3 - 2] によって、不定方程式 $aX + bY = k$ は必ず整数解を持つ。そして、不定方程式 $aX + bY = d$ の 1 つの整数解から、次の命題のようにして、不定方程式 $aX + bY = k$ のすべての整数解を求めることができる。

命題 2 - 2 - 2
a, b を 0 でない整数とし、k を $d = \gcd(a, b)$ の倍数とする。このとき、不定方程式 $aX + bY = k$ は解を持つ。さらに、$(X, Y) = (x_0, y_0)$ を不定方程式 $aX + bY = d$ の 1 つの整数解とすると、不定方程式 $aX + bY = k$ のすべての整数解は次式によって与えられる：

$$(X, Y) = \left(\frac{k}{d} x_0 + \frac{b}{d} t,\ \frac{k}{d} y_0 - \frac{a}{d} t \right) \qquad (t \in \mathbb{Z}).$$

(**証明**)
• 不定方程式 $aX + bY = k$ が解を持つこと：
[系 1 - 3 - 2] により、不定方程式 $aX + bY = d$ は整数解を持つ。その整数解を $(X, Y) = (x_0, y_0)$ とすると、次式が成り立つ：

$$(\diamond) \qquad ax_0 + by_0 = d.$$

一方、k は d の倍数なので、$k = dm$ となる $m \in \mathbb{Z}$ が存在する。$(\diamond)$ の両辺を m 倍して、等式

$$(\sharp) \qquad a(x_0 m) + b(y_0 m) = dm = k$$

得る。よって、不定方程式 $aX + bY = k$ は整数解 $(X, Y) = (x_0 m, y_0 m)$ を持つ。
• 不定方程式 $aX + bY = k$ のすべての整数解を求めること：
$(X, Y) = (x, y)$ を不定方程式 $aX + bY = k$ の整数解とすると、$ax + by = k$ が満たされる。この等式から等式 $(\sharp)$ の各辺を引くと等式

$$(\star) \qquad a(x - x_0 m) + b(y - y_0 m) = 0$$

が得られる。$d = \gcd(a, b)$ であるから、互いに素な整数 a', b' を使って、$a = da',\ b = db'$ と表わすことができる。このとき、$(\star)$ の両辺を d で割り、後ろの項を移項すると、

$$a'(x - x_0 m) = b'(y_0 m - y)$$

が得られる。これより、$a' | b'(y_0 m - y)$ がわかるが、$\gcd(a', b') = 1$ なので、$a' | (y_0 m - y)$ である ([系 1 - 3 - 3(1)])。よって、

$$y_0 m - y = ta' \qquad (t \in \mathbb{Z})$$

とおくことができる。これを $a'(x - x_0 m) = b'(y_0 m - y)$ に代入し、両辺を a' で割って、$x - x_0 m = b't$ が得られる。こうして、$(X, Y) = (x, y)$ が不定方程式 $aX + bY = k$ の整数解であれば、

$$(x, y) = (x_0 m + tb',\ y_0 m - ta') = \left(\frac{k}{d} x_0 + \frac{b}{d} t,\ \frac{k}{d} y_0 - \frac{a}{d} t \right) \qquad (t \in \mathbb{Z})$$

と表わされることがわかった。逆に、上の形をした整数の組が不定方程式 $aX + bY = k$ の解になっていることは容易に確かめられる。 □

例 2 - 2 - 3 不定方程式 $20X + 9Y = 2$ の整数解をすべて求めよ。
解；
2 は $\gcd(20, 9) = 1$ の倍数であるから、不定方程式 $20X + 9Y = 2$ は整数解を持つ。(ユークリッドの互除法を用いることにより、) 不定方程式 $20X + 9Y = 1$ の 1 つの解として $(X, Y) = (-4, 9)$ が見つかる。よって、不定方程式 $20X + 9Y = 2$ の整数解は次で与えられる ([命題 2 - 2 - 2])：

$$(X, Y) = (2 \cdot (-4) + 9t,\ 2 \cdot 9 - 20t) = (-8 + 9t,\ 18 - 20t) \qquad (t \in \mathbb{Z}).$$ □

演習 2-2* 不定方程式 $36X - 100Y = 32$ は解を持つかどうかを調べよ。持つ場合にはその解をすべて求めよ。

● 2 - 3 : 素数

$p \in \mathbb{N}$ が**素数** (prime number) であるとは、$p \neq 1$ であって、1 と p 自身以外に正の約数を持たないときをいう。1 でも素数でもない自然数を**合成数** (composite number) という。例えば、$2, 3, 5, 7, 11$ は素数、$4, 6, 8, 9, 10$ は合成数である。要するに、合成数とは $n = ab$ $(a, b \in \mathbb{N},\ a, b > 1)$ のように、2 つの 2 以上の自然数の積に分解できる数 n のことである。

[系 1 - 3 - 3(1)] から次が導かれる。

補題 2 - 3 - 1

p を素数とする。整数 s, t に対して次が成り立つ：

$$p|st \implies p|s \text{ または } p|t.$$

(**証明**)

$\gcd(p, s) = 1$ ならば、[系 1 - 3 - 3(1)] より、$p|t$ が従う。

$\gcd(p, s) \neq 1$ ならば、$d = \gcd(p, s)$ とおくと、$d(> 1)$ は p の約数である。p は素数だから、$d = p$ とわかる。したがって、p は s の約数であり、$p|s$ が成り立つ。 □

上の補題を繰り返し用いて次が示される。

系 2 - 3 - 2

p を素数とする。整数 $s_1, \ldots, s_k$ に対して次が成り立つ：

$$p|(s_1 \cdots s_k) \implies \exists\, i \in \{1, \ldots, k\} \text{ s.t. } p|s_i.$$

● 2 - 4 : 素因数分解の可能性と一意性

素因数分解の一意性に関する定理は整数論の基本定理と呼ばれている。証明には数学的帰納法が使われる。

定理 2 - 4 - 1 (**素因数分解の可能性と一意性**)

1 以外の任意の自然数 n は、素数の冪の積として次のように表わすことができる：

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}. \tag{2 - 4 a}$$

ここで、$k \geq 1$ であり、$p_1, p_2, \ldots, p_k$ は相異なる素数、$e_1, e_2, \cdots, e_k$ は自然数である。さらに、この表わし方は、$p_1^{e_1}, p_2^{e_2}, \ldots, p_k^{e_k}$ の並べ方の順番を除いて一意的である。(2 - 4 a) の表示を n の**素因数分解** (prime decomposition) といい、$p_1, p_2, \ldots, p_k$ のことを n の**素因数** (prime factor) という。

(**証明**)

I. 素因数分解の可能性：証明は演習問題とする。

Ⅱ. 書き表わし方の一意性：数学的帰納法で証明する。

第 1 段 ($n = 2$ のとき)：2 は素数であるから、これを 2 個以上の素数の積として表わすことはできない。よって、2 を素数の積に書き表わす仕方は唯一通りである。

第 2 段：n を $n > 2$ なる自然数とし、n よりも小さい 2 以上の任意の自然数については、素数の積への書き表わし方は (順番を無視すれば) 一意的であると仮定する。

• n が素数の場合：第 1 段と同様の理由で、n を素数の積に書き表わす仕方は一意的である。

• n が合成数の場合：n が素数の積に次のように 2 通りの仕方で書き表わされたと仮定する (n は合成数なので、下記の表示で、$r, s \geq 2$ に注意)。

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \qquad (p_1, \ldots, p_r, q_1, \ldots, q_s \text{ は素数})$$

このとき、もし、q_1 が $p_1,\ p_2, \ldots, p_r$ のどれかと一致することが示されれば、$\frac{n}{q_1} \in \mathbb{N}$ に帰納法の仮定を用いて、$r = s$ であって、かつ、順番を適当に並べ変えると $p_1 = q_1, p_2 = q_2, \ldots, p_r = q_r$ となることがわかる。

さて、q_1 は素数であり、$q_1 | p_1 p_2 \cdots p_r$ を満たす。[系 2 -3 -2] より、$q_1 | p_i$ となる $i \in \{1, 2, \ldots, r\}$ が存在する。p_i, q_1 はともに素数であるから、$p_i = q_1$ でなければならない。これで、帰納法が完成し、一意性の証明が終わった。 □

● 2 - 5 ： 素因数分解を用いた最大公約数の求め方

2 つの整数 $m, n\ (\geq 2)$ の素因数分解が次のように求められたとしよう。

$$m = p_1^{e_1} \cdots p_k^{e_k},$$
$$n = p_1^{f_1} \cdots p_k^{f_k}.$$

但し、$p_1, \ldots, p_k$ は相異なる素数であり、$e_1, \ldots, e_k$ および $f_1, \ldots, f_k$ の中には 0 があってもよいことにする。このとき、m, n の最大公約数 d は

$$d = p_1^{\min\{e_1, f_1\}} \cdots p_k^{\min\{e_k, f_k\}}$$

により求まる。例えば、24948 と 12870 は $24948 = 2^2 \cdot 3^4 \cdot 7 \cdot 11,\ 12870 = 2 \cdot 3^2 \cdot 5 \cdot 11 \cdot 13$ のように素因数分解されるので、$\gcd(24948, 12870) = 2 \cdot 3^2 \cdot 11 = 198$ と求まる。

演習 2-3　2 つの整数 8568, 7644 をそれぞれ素因数分解して最大公約数を求めよ。また、ユークリッドの互除法を用いて 8568, 7644 の最大公約数を求め、同じ結果になることを確認せよ。

エラトステネス (Eratosthenes, B.C.275〜B.C.194) の篩（ふるい）

小さな整数に対しては、それが素数なのか合成数なのかは簡単にわかる。しかし、値が大きくなるとすぐには判定がつかない。このようなとき、「エラトステネスの篩」として古くから知られている方法を使うと判定することができる。エラトステネスのふるいは 2 からある決めた整数までの間の素数をすべて見つけ出すための方法である。具体的には次のようにする。

2 から 99 までの間の素数を見つけたいとしよう。まず、紙に 2 から 99 までの数字を右のように書き並べる。次に、2 を残して 2 の倍数を全て消す。次に、3 を残して 3 の倍数を全て消す。4 は消されているので素数ではない。5 は消されていないので素数であり、5 を残して 5 の倍数を全て消す。このような操作を 9 ($n^2 > 99$ となる n の一つ手前の数字) まで続ける。すると、消されずに残った数がすべて素数である。

		2	**3**	~~4~~	**5**	~~6~~	**7**	~~8~~	~~9~~
~~10~~	**11**	~~12~~	**13**	~~14~~	~~15~~	~~16~~	**17**	~~18~~	**19**
~~20~~	~~21~~	~~22~~	**23**	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	**29**
~~30~~	**31**	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	**37**	~~38~~	~~39~~
~~40~~	**41**	~~42~~	**43**	~~44~~	~~45~~	~~46~~	**47**	~~48~~	~~49~~
~~50~~	~~51~~	~~52~~	**53**	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	**59**
~~60~~	**61**	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	**67**	~~68~~	~~69~~
~~70~~	**71**	~~72~~	**73**	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	**79**
~~80~~	~~81~~	~~82~~	**83**	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	**89**
~~90~~	~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	**97**	~~98~~	~~99~~