整数について

1　公約数・公倍数

まず，整数を自然数で割ったときの，商・余りとは何かについて述べる。

定理 1.1（割算の定理）

a を整数，b を自然数とするとき

$$a = bh + r, \quad 0 \leqq r < b$$

となる整数の組 $(h,\ r)$ がただひとつ存在する。
この h を a を b で割った商，r を余り（剰余）という。

b の倍数を順番に並べると

$$\cdots, -2b,\ -b,\ 0,\ b,\ 2b,\ \cdots$$

となる。従って

$$bh \leqq a < b(h+1) \cdots ①$$

となる h が存在する。そこで $r = a - bh$ とおく。$a = bh + r$ であり，また ① より $bh \leqq bh + r < b(h+1)$ であるから $0 \leqq r < b$ となる。よって，確かに $a = bh + r, \quad 0 \leqq r < b$ となる整数の組 $(h,\ r)$ が存在する。

次に，一意性を示そう。

$$a = bh_1 + r_1, \quad 0 \leqq r_1 < b \cdots ②$$

$$a = bh_2 + r_2, \quad 0 \leqq r_2 < b \cdots ③$$

とする。②− ③より $0 = b(h_1 - h_2) + r_1 - r_2$ つまり $r_1 - r_2 = b(h_2 - h_1) \cdots ④$となるので $r_1 - r_2$ は b の倍数である。しかし，$0 \leqq r_1 < b, \quad 0 \leqq r_2 < b$ であるから $-b < r_1 - r_2 < b$ である。よって $r_1 - r_2 = 0$ つまり $r_1 = r_2$ となる。そうすると ④ より $b(h_2 - h_1) = 0$ であるが，$b \neq 0$ であるから $h_2 = h_1$ となり $(h_1,\ r_1) = (h_2,\ r_2)$ である。

これで一意性も示された。■

自然数 $a,\ b$ の正の公倍数のうち最小のものを a と b の最小公倍数[注1]という。また $a,\ b$

[注1] Least Common Measure の頭文字をとって LCM と書く。

の公約数のうち最大のものを a と b の最大公約数[注2]という。公倍数・公約数に関して，次の定理は基本である。

定理 1.2（公倍数・公約数）

(1) 公倍数は最小公倍数の倍数である。
(2) 公約数は最大公約数の約数である。

(1) n を a, b の公倍数とし，l を最小公倍数とする。n を l で割った商を h，余りを r とすると $n = lh + r, \quad 0 \leqq r < l$。$r = n - lh$ であるが，n も l も a の倍数であるから $n = an_1,\ l = al_1$ とおくと $r = an_1 - al_1h = a(n_1 - l_1h)$ となり，r も a の倍数である。同様に r は b の倍数にもなる。よって r は a, b の公倍数となる。ここで $r \neq 0$ とすると，r は l より小さい正の公倍数となり，l は正の公倍数のうち最小のものであることに反する。よって $r = 0$ でなければならない。従って $n = lh$ となり，n は l の倍数である。

(2) n を a, b の公約数とし，d を最大公約数とする。$a = na_1,\ a = da_2$ と書けるから a は n と d の公倍数である。そこで n と d の最小公倍数を l とおくと (1) より a は l の倍数であり $a = la_3$ と書ける。
同様に，b も n と d の公倍数であるから，l の倍数となり $b = lb_3$ と書ける。
従って，l は a と b の公約数となる。しかし，公約数の中で最大のものが d であるから $l \leqq d \cdots$①となる。
一方 l は n と d の（最小）公倍数であったから，特に l は d の倍数であり $d \leqq l \cdots$② となる。
① と ② より $l = d$ である。以上で n と d の最小公倍数は d であることが分かった。これは n が d の約数であることを意味している。■

最小公倍数と最大公約数の関係は次の定理から分かる。

定理 1.3

自然数 a, b の最小公倍数を l，最大公約数を d とすると $ab = ld$ である。

ab は a, b の公倍数なので 定理 1.2(1) より $ab = lm \cdots$①と書ける。一方 l は $a,\ b$ の公倍数なので $\begin{cases} l = al_1 & \cdots ② \\ l = bl_2 & \cdots ③ \end{cases}$ と書ける。② を ① に代入すると $ab = mal_1$ となり $b = ml_1 \cdots ④$ を得る。同様に ③ を ① に代入すると $ab = mbl_2$ となり $a = ml_2 \cdots ⑤$を得る。④ と ⑤ より m は a と b の公約数である。そうすると，定理 1.2(2) より m は最大公約数 d の約数

[注2] Greatest Common Divisor の頭文字をとって GCD と書く。

であるから $d = me \cdots ⑥$ と書ける。

一方，d は a の約数であるから $a = da_1$ と書ける。これと ⑤ より $ml_2 = da_1$ となる。ここへ ⑥ を代入すると $ml_2 = mea_1$ となり $l_2 = ea_1 \cdots ⑦$ を得る。また d は b の約数であるから $b = db_1$ と書ける。これと ④ より $ml_1 = db_1$ となる。ここへ ⑥ を代入すると $ml_1 = meb_1$ なり $l_1 = eb_1 \cdots ⑧$ を得る。⑦ を ③ へ代入すると $l = bea_1$，⑧ を ② へ代入すると $l = aeb_1$ となる。よって $l = e(ba_1) = e(ab_1)$ となり $\dfrac{l}{e} = ba_1 = ab_1$ で，自然数 $\dfrac{l}{e}$ は a, b の公倍数である。ここでもし，$e > 1$ とすると 自然数 $\dfrac{l}{e}$ は l より小さい正の公倍数であるから l が最小公倍数であることに反する。よって $e = 1$ である。そうすると ⑥ より $d = m$ である。これを ① に代入すると $ab = ld$ となる。■

上に述べた定理を用いると，実際に整数の問題を解くときによく使う次の定理を示すことが出来る。

定理 1.4

ab が c で割り切れ，しかも b と c が互いに素ならば，a は c で割り切れる。

b と c は互いに素であるから b と c の最大公約数は 1 である。よって 定理 1.3 より bc は b と c の最小公倍数となる。ところが仮定より ab は c の倍数であり，また ab は b の倍数でもあるから ab は c と b の公倍数である。よって，定理 1.2 より ab は b と c の最小公倍数 bc の倍数である。従って $ab = bch$ と書ける。よって $a = ch$ となり a は c で割り切れる。■

2 素数

自然数 p が 1 と p 以外に正の約数を持たないとき，p を素数という。$2, 3, 5, 7, 11, \cdots$ は素数である。

次の定理は素数を特徴付ける重要な定理である。

定理 2.1（素数の特徴付け）

a, b を自然数とし，p を素数とする。このとき
ab が p で割り切れるなら，a または b のうち少なくとも一方は，p で割り切れる。

a と p の最大公約数を d とおく。d は p の約数であるが，p は素数であるから $d = 1$ ま

たは $d = p$ である。

もし $d = p$ なら a は p で割り切れる。また $d = 1$ なら a と p は互いに素である。そして ab は p で割り切れるから，定理 1.4 より b が p で割り切れる。■

上の定理を一般化して，次を示すことも出来る。

系 2.2

$n \geqq 2$ とし，$a_1,\ a_2,\ \cdots,\ a_n$ を自然数とする。
$a_1a_2\cdots a_n$ が素数 p で割り切れるなら，$a_1,\ a_2,\ \cdots,\ a_n$ のうち少なくともひとつは，p で割り切れる。

n に関する数学的帰納法で示す。

$n = 2$ のときは，定理 2.1 で示されている。

$n = k$ のとき正しいと仮定して，$n = k + 1$ のときに考える。

$a_1a_2\cdots a_{k+1} = (a_1a_2\cdots a_k)a_{k+1}$ が p で割り切れるので，定理 2.1 より $a_1a_2\cdots a_k$ または a_{k+1} が p で割り切れる。a_{k+1} が p で割り切れるなら示すことは何もない。$a_1a_2\cdots a_k$ が p で割り切れるときは，帰納法の仮定から $a_1,\ a_2,\ \cdots,\ a_k$ のうち少なくともひとつは，p で割り切れる。よっていずれにせよ，$a_1,\ a_2,\ \cdots,\ a_{k+1}$ のうち少なくともひとつは，p で割り切れることになり，$n = k + 1$ のときも正しくなる。

以上で，n に関する数学的帰納法で示された。■

これを用いると，素因数分解の可能性・一意性が証明できる。

定理（素因数分解）

2 以上の自然数は，素数の積に表すことができる。
しかも，その表し方は，積の順序を除いて一意的である。

（★）n を 2 以上の自然数とするとき n は素数の積に表される
ことを n に関する数学的帰納法で示す。

$n = 2$ のときは 2 が素数であるから正しい。

$n \leqq k$ のとき正しい仮定して $n = k + 1$ のときに考える。

もし，$k + 1$ が素数なら示すことはない。

$k + 1$ が素数でないなら 1 と $k + 1$ 以外に正の約数 a を持ち $k + 1 = ab\cdots$① と書ける。
$a \neq 1,\quad a \neq k + 1$ であるから $2 \leqq a < k + 1,\quad 2 \leqq b < k + 1$ つまり $2 \leqq a \leqq k,\quad 2 \leqq b \leqq k$ である。よって帰納法の仮定から a も b も素数の積に表される。これを ① に代入すると $k + 1$ が素数の積に表されることになる。よって，いずれにせよ $n = k + 1$ のときも （★）

は正しくなり帰納法によって示された。

次に
（☆）n を 2 以上の自然数とするとき n を素数の積に表す表し方は一意的である
ことを n に関する帰納法で示す。
$n = 2$ のときは 2 が素数であるから正しい。
$n \leqq k$ のとき正しい仮定して $n = k + 1$ のときに考える。

$$k + 1 = p_1 p_2 \cdots p_l = q_1 q_2 \cdots q_m \cdots ② \quad (p_i,\ q_j \text{ は素数})$$

を，ともに素数の積への分解とする。p_1 は $q_1 q_2 \cdots q_m$ を割り切るが p_1 は素数であるから 系 2.2 より $q_1, q_2, \cdots, q_m$ のうち少なくともひとつは p_1 で割り切れる。例えば，q_1 が p_1 で割り切れるとすると，q_1 も素数であるから $q_1 = p_1$ となる。よって ② より $p_2 p_3 \cdots p_n = q_2 q_3 \cdots q_m$ となる。ここで $x = p_2 p_3 \cdots p_n = q_2 q_3 \cdots q_m$ とおくと $x < k + 1$ つまり $x \leqq k$ であるから，帰納法の仮定より x を素数の積に表す表し方は一意的であり，$p_2 p_3 \cdots p_n$ と $q_2 q_3 \cdots q_m$ は同じ分解である。従って $p_1 p_2 \cdots p_l$ と $q_1 q_2 \cdots q_m$ は同じ分解となり $n = k + 1$ のときも（☆）は正しくなり帰納法によって示された。■

3 Euclid の互除法

次の定理は整数の問題を考えるときの基本となる定理である。

定理 3.1

自然数 $a,\ b$ の最大公約数を d とするとき $am + bn = d$ となる整数 $m,\ n$ が存在する。
特に，a と b が互いに素のときは $am + bn = 1$ となる整数 $m,\ n$ が存在する。

$S = \{ax + by \mid x, y \text{ は整数}\}$ とおく。S に含まれる正の整数で最小のものを k とし，$k = am + bn \cdots ①$とおく。d は $a,\ b$ の最大公約数であるから $a = da_0,\ b = db_0$ と書ける。これを ① に代入すると $k = da_0 m + db_0 n = d(a_0 m + b_0 n)$ となるから k は d の倍数である。一方，$a = a \cdot 1 + b \cdot 0$，$b = a \cdot 0 + b \cdot 1$ であるから $a,\ b \in S$ である。a を k で割った商を h，余りを r とすると $a = hk + r\ (0 \leqq r < k)$ となる。ここへ ① を代入すると $a = h(am + bn) + r$ つまり $r = a(1 - hm) + b(-hn)$ となり $r \in S$ である。ここでもし $r > 0$ なら k より小さい正の整数で S に含まれるものが存在することとなり k の最小性に反する。よって $r = 0$ であり，k は a の約数である。同様にして k は b の約数でもあり，従って k は $a,\ b$ の公約数となる。しかし，最初に見たように k は，$a,\ b$ の最大公約数の倍数でもある。公約数でしかも最大公約数の倍数でもあるものは最大公約数だけであるから，結局 $k = d$ となり $am + bn = d$ である。以上で示された。■

$a,\ b$ が大きい数のときには，上の定理の d や $m,\ n$ を簡単に求めることは出来ない。次に述べる Euclid の互除法は，自然数 $a,\ b$ が与えられたとき $a,\ b$ の最大公約数を求める便利な方法である。また，この方法を利用すれば，$a,\ b$ の最大公約数を d とするとき $am + bn = d$ となる整数 $m,\ n$ を機械的に求めることができる。

まず，準備として次を示す。

命題 3.2

自然数 $p,\ q,\ h,\ r$ が $p = qh + r \cdots ①$を満たすとき
p と q の公約数の全体と，q と r の公約数の全体は一致する。
特に，p と q の最大公約数と，q と r の最大公約数は一致する。

s を p と q の公約数とすると $p = sp_1,\ q = sq_1$ と書ける。これを ① に代入すると $sp_1 = sq_1h + r$ となる。よって $r = s(p_1 - q_1h)$ となるので，s は r の約数でもある。そして，もともと s は q の約数でもあったから，q と r の公約数となる。

一方，t を q と r の公約数とすると $q = tq_2,\ r = tr_1$ と書ける。これを ① に代入すると $p = tq_2h + tr_1$ となる。よって $p = t(q_2h + r_1)$ となるので，t は p の約数でもある。そして，もともと t は q の約数でもあったから，p と q の公約数となる。

また，最大公約数とは，公約数の中で最も大きいもののことであるから，公約数の全体が一致すれば最大公約数も一致する。■

$a,\ b$ の最大公約数を $(a,\ b)$ で表わすことにする。
$(a,\ b)$ を求める方法を述べる。

まず，a を b で割って，その商を h_1，余りを r_1 とする。

$$a = bh_1 + r_1 \quad (0 \leqq r_1 < b)$$

次に，b を r_1 で割って，その商を h_2，余りを r_2 とする。

$$b = r_1h_2 + r_2 \quad (0 \leqq r_2 < r_1)$$

今度は，r_1 を r_2 で割って，その商を h_3，余りを r_3 とする。

$$r_1 = r_2h_3 + r_3 \quad (0 \leqq r_3 < r_2)$$

以下この操作を繰り返す。そのとき，いつかは余りが 0 となってこの操作が終わることに注意する。実際，もし無限にこの操作が続くとすると，余りの無限列 $b > r_1 > r_2 > r_3 > \cdots \geqq 0$ が得られることになる。 しかし，b と 0 の間には有限個の自然数しか存在しないので矛盾である。

そこで

$$r_{n-1} = r_n h_{n+1} + r_{n+1} \quad (0 \leqq r_{n+1} < r_n)$$

$$r_n = r_{n+1} h_{n+2} \quad (r_{n+2} = 0)$$

となって，操作が完了したとする。そうすると上の命題によって

$$(a,\ b) = (b,\ r_1) = (r_1,\ r_2) = \cdots = (r_n,\ r_{n+1})$$

となる。しかし，更に $r_n = r_{n+1} h_{n+2}$ であるから r_n と r_{n+1} の最大公約数は r_{n+1} である。つまり $(r_n,\ r_{n+1}) = r_{n+1}$ となる。従って

$$(a,\ b) = r_{n+1}$$

と分かる。つまり順々に余りで割っていくとき，割り切れる直前の余りが最大公約数である。この操作を Euclid の互除法と言う。

［例］$(1996,\ 308)$ を求める。順々に割っていくと

$$1996 = 308 \cdot 6 + 148$$
$$308 = 148 \cdot 2 + 12$$
$$148 = 12 \cdot 12 + 4$$
$$12 = 4 \cdot 3$$

となる。よって $(1996,\ 308) = 4$ である。

さて $(a,\ b) = d$ とすると，互除法の操作で

$$a = bh_1 + r_1 \cdots ①$$
$$b = r_1 h_2 + r_2 \cdots ②$$
$$r_1 = r_2 h_3 + r_3 \cdots ③$$
$$\cdots\cdots$$
$$r_{n-1} = r_n h_{n+1} + d \cdots ④$$
$$r_n = d h_{n+2}$$

となる。ここで，各余り r_j は $a,\ b$ を用いて表わせることに注意する。
①より

$$r_1 = a - bh_1 \cdots ⑤$$

であるから，これを ② に代入すると

$$r_2 = b - (a - bh_1)h_2 \cdots ⑥$$

となる。次に ⑤ ⑥ を ③ に代入すると

$$r_3 = a - bh_1 - \{b - (a - bh_1)h_2\}h_3$$

となる。以下この操作を繰り返していくと，最終的には r_{n-1}，r_n を a, b で表わしたものを ④ に代入すると

$$d = am + bn$$

の形の式を得る。

［例］$(1996,\ 308) = 4$ であったので $1996m + 308n = 4$ となる m, n を求めてみる。

$1996 = 308 \cdot 6 + 148 \cdots ①$
$308 = 148 \cdot 2 + 12 \cdots ②$
$148 = 12 \cdot 12 + 4 \cdots ③$

① より

$$148 = 1996 - 308 \cdot 6 \cdots ④$$

である。 ④ を ② に代入すると

$$12 = 308 - (1996 - 308 \cdot 6) \cdot 2 \cdots ⑤$$

となる。そこで ④ ⑤ を ③ に代入すると

$$4 = 1996 - 308 \cdot 6 - \{308 - (1996 - 308 \cdot 6) \cdot 2\} \cdot 12$$

となる。これを整理すると

$$1996 \cdot 25 - 308 \cdot 162 = 4$$

を得る。