講義資料 (4): 約数・倍数，ユークリッドの互除法

4.1 整数の基本性質

本節は，教科書 3.1 節の最初の部分 (pp.101–106) に対応する．

定義 4.1 整数上の関係 | を以下で定義する．

$$n|m \iff^{\text{def}} \exists k \in \mathbb{Z}.\ kn = m$$

$n|m$ であるとき，m は n の**倍数** (multiple) である，または，n は m の**約数** (divisor) であると呼ぶ．なお，$n|m$ でないことを $n \not| m$ で記す． □

NOTE: 定義より，1 と -1 は全ての整数の約数であり，0 は全ての整数の倍数である．

定義 4.2 整数 n の**絶対値** (absolute value) を $|n|$ で記し，以下で定義する．

$$|n| \stackrel{\text{def}}{=\!=} \begin{cases} n & \text{if } n \geq 0 \\ -n & \text{if } n < 0 \end{cases}$$ □

定理 4.3 (剰余定理) $m, n \in \mathbb{Z}$ で $n \neq 0$ とすると，次式を成立させる整数 q, r が一意に存在する．

$$m = qn + r, \quad 0 \leq r < |n| \qquad \cdots\cdots(\alpha)$$

証明 最初に，(α) を満たす整数 q, r が存在することを示す．

(I) $m \geq 0$ かつ $n > 0$ とする．
m に関する帰納法で (α) を満たす整数 q, r が存在することを示す．

Basis $m = 0$ とする．$q = r = 0$ とすると (α) が成立．

I.S. $m > 0$ とする．

(i) $n > m$ の場合を考える．$m = 0 \cdot n + m$ と $0 \leq m < |n|$ より，$q = 0$ かつ $r = m$ とすれば良い．

(ii) $n \leq m$ の場合を考える．$m' = m - n$ とすると，$n > 0$ より $0 \leq m' < m$．よって，帰納法の仮定より，ある整数 q', r' が存在して $m' = q'n + r'$ かつ $0 \leq r' < |n|$．$m = m' + n = (q' + 1)n + r'$ であるので，$q = q' + 1$，$r = r'$ とすれば良い．

(II) $m < 0$ かつ $n > 0$ とする．
(I) より，ある整数 q', r' が存在して $-m = q'n + r'$ かつ $0 \leq r' < |n|$．$r' = 0$ の場合は $m = (-q')n + 0$ であるので，$q = -q', r = 0$ とすれば良い．$r' > 0$ とする．このとき，$m = -q'n - r' = (-q' - 1)n + (n - r')$．ここで，$0 < r' < |n| = n$ であるので $0 \leq n - r' < |n|$．よって，$q = -q' - 1$，$r = n - r'$ とすれば (α) が成立．

(III) $n < 0$ とする．

(I,II) より，ある整数 q', r' が存在して $m = q'(-n) + r'$ かつ $0 \leq r' < |n|$．このとき，$m = (-q')n + r'$．よって，$q = -q'$，$r = r'$ とすれば (α) が成立．

次に，(α) を満たす整数 q, r の一意性を示す．ある整数 q_i, r_i $(i = 1, 2)$ が存在して，各 i で $m = q_i n + r_i$ かつ $0 \leq r_i < |n|$ が成立するとする．このとき，$q_1 = q_2$ かつ $r_1 = r_2$ であることを示せば十分．

$(q_1 - q_2)n = r_2 - r_1$ であるので，$r_2 - r_1$ は n の倍数．ここで，各 i で $0 \leq r_i < |n|$ となるので，$0 \leq |r_2 - r_1| < |n|$．よって，$r_2 - r_1 = 0$，すなわち $r_1 = r_2$ となる．また，$(q_1 - q_2)n = r_2 - r_1$ に $r_1 = r_2$ を代入すると，$(q_1 - q_2)n = 0$ となる．ここで，$n \neq 0$ なので，$q_1 - q_2 = 0$，すなわち $q_1 = q_2$ となる． □

定義 4.4 $m, n \in \mathbb{Z}$ で $n \neq 0$ とする．定理 4.3 より，$m = qn + r$ かつ $0 \leq r < |n|$ となる整数 q, r が一意に存在する．このとき，q と r をそれぞれ，m を n で割った**商** (quotient) および**剰余** (remainder) と言う．また，商および剰余を求める (中置) 演算を div , mod で記す． □

例えば $13 \bmod 4 = 1$, $13 \operatorname{div} 4 = 3$ となる．ここで，$m \bmod n$ や $m \operatorname{div} n$ は，$n = 0$ のとき値が未定義となってることに注意されたし．

NOTE: 通常のプログラム言語における商演算や剰余演算の定義は，負の値に対しては上述の div や mod と異なる場合が多い．注意されたし．

4.2 公約数と公倍数

本節は，教科書 3.1 節の中程 (pp.113–114) に対応する．

定義 4.5 整数 d が二つの整数 m, n の両方の約数であるとき，d を m と n の**公約数** (common divisor) といい，整数 l が二つの整数 m, n の両方の倍数であるとき，l を m と n の**公倍数** (common multiple) という． □

定義 4.6 m, n を 0 でない整数とする．m と n の正の公約数のうち最大の正整数を m と n の**最大公約数** (greatest common divisor) と呼び，$\gcd(m, n)$ で記す (単に (m, n) と記すこともある)．また，m と n の正の公倍数のうち最小の正整数を m と n の**最小公倍数** (least common multiple) と呼び，$\operatorname{lcm}(m, n)$ で記す．また，便宜上 0 に対しては $\gcd(m, 0) = \gcd(0, m) = |m|$，$\operatorname{lcm}(m, 0) = \operatorname{lcm}(0, m) = 0$ と考える．特に，$\gcd(m, n) = 1$ であるとき，m と n は**互いに素** (mutually indivisible) であるという． □

ここで，最大公約数の概念を任意個数の整数を同時に取り扱えるように拡張しておく．

定義 4.7 整数 $a_1, a_2, \ldots, a_n$ の最大公約数を，全ての a_i が 0 で無い場合は定義 4.6 と同様に定義し $\gcd(a_1, a_2, \ldots, a_n)$ で記す (以下では単に $(a_1, a_2, \ldots, a_n)$ で記す)．また，いずれかの i で $a_i = 0$ となっている場合は，便宜上以下のように考える．

$$\begin{aligned} (a_1, \ldots, a_{i-1}, 0, a_{i+1}, \ldots, a_n) &= (a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n) \\ (0, \ldots, 0) &= 0 \end{aligned}$$

□

補題 4.8 $a_1, \ldots, a_n$ を整数とする．各 i で，任意の整数 $t_1, \ldots, t_n$ に対し (ただし $t_i = 0$ とする) 以下の等式が成立.

$$(a_1, a_2, \ldots, a_n) = (a_1 + t_1 a_i,\ a_2 + t_2 a_i, \ldots,\ a_n + t_n a_i)$$

証明 一般性を失う事なく $i = 1$ の場合のみを示す.
最初に，任意の整数 $a_1, \ldots, a_n, t_2, \ldots, t_n$ に対し以下の不等式が成立することを示す.

$$(a_1, a_2, \ldots, a_n) \leq (a_1,\ a_2 + t_2 a_1, \ldots,\ a_n + t_n a_1) \qquad \cdots\cdots (\alpha)$$

$(a_1, \ldots, a_n) = d$ とする．$d = 0$ のときは $a_1 = \cdots = a_n = 0$ となるので明らかに (α) は成立.
$d \neq 0$ とする．各 j (≥ 2) で，$\frac{a_j + t_j a_1}{d} = \frac{a_j}{d} + t_j \frac{a_1}{d} \in \mathbb{Z}$ なので，d は $a_2 + t_2 a_1,\ \ldots,\ a_n + t_n a_1$ の公約数．最大公約数の定義より $d \leq (a_1,\ a_2 + t_2 a_1,\ \ldots,\ a_n + t_n a_1)$．以上より，$(\alpha)$ が示せた.
ここで，(α) が任意の整数 $a_1, \ldots, a_n, t_2, \ldots, t_n$ に対し成立することに注意して，(α) を繰り返し適用することにより以下を得る.

$$\begin{aligned}(a_1, \ldots, a_n) &\leq (a_1,\ a_2 + t_2 a_1, \ldots,\ a_n + t_n a_1) \\ &\leq (a_1,\ (a_2 + t_2 a_1) - t_2 a_1, \ldots,\ (a_n + t_n a_1) - t_n a_1) \\ &= (a_1, \ldots, a_n)\end{aligned}$$

よって，$(a_1, a_2, \ldots, a_n) = (a_1,\ a_2 + t_2 a_1, \ldots,\ a_n + t_n a_1)$. □

補題 4.9 任意の整数 m, n に対し $(m, n) = (n, m) = (n, m - n)$ が成立．さらに，$n \neq 0$ ならば $(m, n) = (n, m \bmod n)$ も成立.

証明 最大公約数の定義より $(m, n) = (n, m)$．補題 4.8 より，$(n, m) = (n, m - n)$.
$n \neq 0$ とし，$q = m \operatorname{div} n$，$r = m \bmod n$ とする．このとき，$m = qn + r$ が成立している.
補題 4.8 を考えて $(m, n) = (n, m) = (n, m - qn) = (n, r) = (n, m \bmod n)$. □

定理 4.10 a, b を $(a, b) = d$ となる整数とすると，ある整数 x, y が存在して $ax + by = d$.

証明 $|b|$ に関する帰納法で示す.

Basis $|b| = 0$ とする．$0 \leq a$ のときは $x = 1$，$a < 0$ のときは $x = -1$ とすると (y はどんな値でも良い)，$ax + by = |a| = (a, 0) = d$.

I.S. $|b| > 0$ とする．剰余定理 (定理 4.3) より，ある整数 q, r が存在して $a = qb + r$ かつ $0 \leq r < |b|$．補題 4.9 より，$(a, b) = (b, r)$．$|r| < |b|$ なので，帰納法の仮定よりある整数 x', y' が存在して $bx' + ry' = d$．よって，$x = y', y = x' - qy'$ とすると $ax + by = ay' + b(x' - qy') = bx' + (a - bq)y' = bx' + ry' = d$. □

補題 4.11 $(a, b) = 1$ かつ $a | bc$ ならば $a | c$.

証明 定理 4.10 より，ある整数 x, y が存在して $ax + by = 1$．よって，$acx + bcy = c$．仮定より $a | bc$ なので，$a | (acx + bcy)$．よって，$a | c$. □

補題 4.12 $a = a'd,\ b = b'd,\ (a,b) = d > 0$ ならば $(a',b') = 1$.

証明 定理 4.10 より，ある整数 x, y が存在して $ax + by = d$．よって，$a'dx + b'dy = d$．$d \neq 0$ なので $a'x + b'y = 1$．ここで，$(a',b') = k$ とする．最大公約数の定義より $0 \leq k$．また，k は a', b' の公約数なので $a'x + b'y$ の約数，すなわち 1 の約数．よって $k = 1$． □

定理 4.13 整数 m, n の最小公倍数を l，最大公約数を d とする．

(1) m, n の任意の公約数 k に対し $k|d$

(2) m, n の任意の公倍数 k に対し $l|k$

(3) $|mn| = dl$

証明 最大公約数の定義より $0 \leq d$，最小公倍数の定義より $0 \leq l$ が成立．

(1) 定理 4.10 より，ある整数 x, y が存在して $mx + ny = d$．ここで，$k|m$ より $k|mx$，また，$k|n$ より $k|ny$．よって，$k|(mx + ny)$．よって，$k|d$.

(2) $l = 0$ とする．このとき $m = 0$ または $n = 0$．0 の倍数は 0 のみなので $k = 0$．よって，$l|k$ が成立．

$l > 0$ とする．剰余定理 (定理 4.3) より，ある整数 q, r が存在して $k = ql + r$ かつ $0 \leq r < l$．ここで，l, k は共に m, n の公倍数なので，r も m, n の公倍数．最小公倍数 l は最小の正の公倍数なので $r = 0$．よって，$k = ql$，すなわち $l|k$.

(3) $d = 0$ とする．このとき，$m = n = 0$．よって，$|mn| = 0 = dl$.

$d > 0$ とする．m, n は共に d の倍数なので，ある整数 m', n' が存在して $m = m'd,\ n = n'd$．補題 4.12 より $(m', n') = 1$．ここで，$l = mk$ とする．$n \mid l$ なので $n'd \mid (m'k)d$ となり，$n'|m'k$ となる．補題 4.11 より $n'|k$．よって，ある整数 t が存在して $k = n't$．$t = 0$ の場合は $k = 0$ となり，$l = 0$ となる．このとき，最小公倍数の定義より $m = 0$ または $n = 0$．よって，$|mn| = 0 = dl$．$t \neq 0$ とする．このとき，$l = mk = mn't$．ここで，$mn' = \frac{mn}{d} = m'n$ なので mn' は m と n の公倍数．l は m と n の最小公倍数なので，$l = mn't$ と $t \neq 0$ より $l = |mn'|$ となる．よって，$l = |mn'| = \frac{|mn|}{d}$，すなわち $ld = |mn|$. □

NOTE: この定理は，素因数分解の概念を用いるともっと簡単に証明できる (次回の資料で説明).

4.3 ユークリッドの互除法

本節は，教科書 3.1 節の最後の部分 (pp.114–116) に対応する．本節では，最大公約数を求めることができる「ユークリッドの互除法」と呼ばれる有名でかつ重要でかつ効率的な手法を紹介する．

アルゴリズム 4.14 (ユークリッドの互除法)
入力として正整数 m, n を受け取り，以下を実行し，$\gcd(m, n)$ を出力する．

$(d, 0)$ の形になるまで対 (m, n) に $\Rightarrow_E$ を繰り返し適用し，
d の値を $\gcd(m, n)$ として出力する．

ただし，$\Rightarrow_E$ は $(x, y) \Rightarrow_E (y, x \bmod y)$ で与えられる．

例 4.15 以下のように，117 と 51 の最大公約数 $\gcd(117, 51)$ をユークリッドの互除法で求めると 3 となる．

$$(117, 51) \Rightarrow_E (51, 15) \Rightarrow_E (15, 6) \Rightarrow_E (6, 3) \Rightarrow_E (3, 0) \qquad \square$$

定理 4.16 任意の正整数 m, n に対してユークリッドの互除法はいつでも出力を得る．また，この出力を r とすると $r = \gcd(m, n)$ が成立する．

証明 $r_0 = m, r_1 = n$ とし，$\Rightarrow_E$ のよる変換の列を $(r_0, r_1) \Rightarrow_E (r_1, r_2) \Rightarrow_E (r_2, r_3) \Rightarrow_E \cdots$ とする．
最初に，ユークリッドの互除法がいつでも出力を得る事を示す．$m = n$ のときは $(m, n) \Rightarrow_E (n, 0)$ なので明らかに出力を得る．$m < n$ のときは $(m, n) \Rightarrow_E (n, m)$ となるので $m > n$ のときのみ示せば十分．各 i で $r_{i+2} = r_i \bmod r_{i+1} < r_{i+1}$ なので $r_0 > r_1 > r_2 > \cdots$ となる．よって，ある $k < r_0$ が存在して $r_{k+1} = 0$ となり，出力 r_k を得る．
次に，ユークリッドの互除法の健全性，すなわち，正整数 m, n に対する出力が $\gcd(m, n)$ となっている事を示す．ユークリッドの互除法が k 回の変換で出力 r_k を得た，すなわち，$(r_0, r_1) \Rightarrow_E \cdots \Rightarrow_E (r_k, 0)$ とする．補題 4.9 と $\Rightarrow_E$ の定義より，$(m, n) = (r_0, r_1) = \cdots = (r_{k-1}, r_k)$ となる．$r_{k-1} \bmod r_k = 0$ であるので，$r_k | r_{k-1}$．よって，$(r_{k-1}, r_k) = r_k$．よって，$(m, n) = r_k$. $\square$

命題 4.17 m, n を $m > n$ となる正整数とし，k を n の 10 進桁数とする．ユークリッドの互除法で m と n の最大公約数を求めるのに必要なステップ数は高々$5k$ ステップである．

証明 (概略のみ示す) l ステップで最大公約数が求まったとする．ここで，$m > n > 0$ なので l は正整数である．
最初に，$\alpha = \frac{1+\sqrt{5}}{2}$ とすると，$\alpha^{l-1} \leq fib(l+1)$ が成立する事を示す (ちなみに，α は黄金比であり，fib は問 4.5 で紹介するフィボナッチ数列)．$l = 1$ のときは明らか．$l \geq 2$ とする．ここで，任意の i に対し，$fib(i)$ は $\frac{\alpha^i}{\sqrt{5}}$ に最も近い整数になることが知られている (証明は割愛)．よって，$fib(l+1) \geq \lceil \frac{\alpha^{l+1}}{\sqrt{5}} \rceil$ ($\lceil x \rceil$ は x より小さくならない最小の整数)．$l \geq 2$ と $\alpha^2 > \sqrt{5}$ より $\lceil \frac{\alpha^{l+1}}{\sqrt{5}} \rceil \geq \lceil \alpha^{l-1} \rceil \geq \alpha^{l-1}$．まとめると，$fib(l+1) \geq \lceil \frac{\alpha^{l+1}}{\sqrt{5}} \rceil \geq \lceil \alpha^{l-1} \rceil \geq \alpha^{l-1}$．
さて，l ステップで m と n の最大公約数が求まったので，$(a_{l+1}, a_l) \Rightarrow_E (a_l, a_{l-1}) \Rightarrow_E \cdots \Rightarrow_E (a_2, a_1) \Rightarrow_E (a_1, 0)$ となる a_i $(i = 1, 2, \ldots, l+1)$ が存在する．ここで，$m = a_{l+1}$ かつ $n = a_l$ であり，$\Rightarrow_E$ は例 4.15 で導入した関係である．このとき，各 i $(1 \leq i \leq n+1)$ で $fib(i+1) \leq a_i$ が成立していることが i に関する帰納法で示せる．よって，$fib(l+1) \leq a_l = n$．n の 10 進桁数が k なので $10^{k-1} \leq n < 10^k$．よって，$fib(l+1) \leq a_l = n < 10^k$．$\alpha^{l-1} \leq fib(l+1)$ なので $\alpha^{l-1} < 10^k$．$\alpha^5 = 11.09\cdots > 10$ なので $(\alpha^{l-1})^5 = (\alpha^5)^{l-1} > 10^{l-1}$．よって，$10^{l-1} < 10^{5k}$ となり $l - 1 < 5k$ となる．l, k は整数なので $l \leq 5k$ を得る． $\square$

演習課題

問 4.1 a, b を $(a, b) = 1$ となる 0 でない整数とする．このとき，$(a, bc) = (a, c)$ となることを素因数分解 (次回の資料で説明) を用いずに示せ．

問 4.2 a, b を $(a, b) = d$ となる 0 でない整数とする．このとき以下の関係が成立することを証明せよ．

$$\{ax + by \mid x, y \in \mathbb{Z}\} = \{dz \mid z \in \mathbb{Z}\}$$

問 4.3 定義 4.1 で与えた関係 $|$ が自然数上の半順序である事を示せ．

NOTE: なお，関係 $|$ は自然数上の半順序ではあるが整数上の半順序ではない．実際，$-1|1$ かつ $1|-1$ が成立するので整数上では反対称性が成立しない．ただし，整数上でも反射性と推移性は成立するので擬順序ではある．

問 4.4 $(4709, 1547)$ の値を素因数分解を用いて求めよ．また，ユークリッドの互除法を用いても求めよ．

問 4.5 フィボナッチ数 (Fibonacci number) の生成関数 fib は以下で定義される．

$$fib(n) \stackrel{\text{def}}{=\!=} \begin{cases} 0 & \text{if } n = 0 \\ 1 & \text{if } n = 1 \\ fib(n-1) + fib(n-2) & \text{if } n > 1 \end{cases}$$

このとき，$n \geq 2$ に対し $(fib(n+1), fib(n))$ をユークリッドの互除法で求めると $n-1$ ステップかかることを，より詳細には以下のような計算過程になることを示せ．

$$(fib(n+1), fib(n)) \Rightarrow_E (fib(n), fib(n-1)) \Rightarrow_E \cdots \Rightarrow_E (fib(3), fib(2)) \Rightarrow_E (1, 0)$$