New Series, No.**Z01**. version Jul. 2011.

整数論の基礎

Article by YAMASHITA, KOICHIRO.

MJKns(2011-) ZahlenTh-01. Mon Jul 18 14:59:53 2011 JST

この document は，過去に公にしたテキストの Appendix (付録) を編集し直したものです．既読の方もいると思いますが，初等整数論の基礎中の基礎に当たる部分です．もう一度，Web 上で accessible にするのも無意味ではなかろう，と思い，MJK New Series の 1 つにすることにしました．
書き直し，編集し直して公にすることを許可してくれた数学科に感謝します．

This document is another version of Appendix in a Classroom Text. I thank the staff of MATH Dptmt. for allowing me to rewrite and publish this on WEB.

MJKNS Z01. Number Theory. file: `mjkNSZ01bt1.pdf`
This file is DLable from `http://kymst.net/mjk`
Articled by `kymst`. Copy Ultra Left. All-Rights ReVERSEd.

Part 1. 除法，素数と Euclid の定理

整数論の基礎である除法と素数，そして Euclid の定理から始めよう．

整数論とは，我々に最もなじみ深い整数 $\mathbb{Z}$，およびその部分集合としての非負整数の集合 $\mathbb{N}$，正整数の集合 $\mathbb{Z}^+$ のもつ数学的構造の研究である．整数の集合 $\mathbb{Z}$ には，加法およびその逆演算としての減法，そして乗法が定義されている．

このように，集合といくつかの演算を組にしたものを**代数系** (*algebraic system*) と呼ぶ．整数は代数系 $\langle \mathbb{Z}; +, \cdot \rangle$ である．特に，加法と乗法について，次が成り立つ：

(i) 加法は結合法則，交換法則をみたす．

(ii) 特別な元 0 が存在して，任意の $x \in \mathbb{Z}$ について $x + 0 = x$ である．この特別な元 0 を「加法の単位元」と呼ぶ．

(iii) 任意の元は加法に関する逆元をもつ．つまり任意の $x \in \mathbb{Z}$ についてそれぞれ $y \in \mathbb{Z}$ が存在して，$x + y = 0$ が成り立つ．この元 y を『x の反元』と言い，通常 $-x$ で表す．

(iv) 乗法は結合法則と交換法則をみたす．

(v) 乗法は加法に関して分配的である．つまり分配法則が成り立つ．

(vi) 乗法の単位元 1 が存在する．

これらの条件をみたす代数系を**単位元をもつ可換環** (*commutative ring with unity*) と言う．従って，整数の集合 $\mathbb{Z}$ は，単位元をもつ可換環である．そこで，$\mathbb{Z}$ を **(有理) 整数環** ((*rational*) *integer ring*) と呼ぶことがある．

1　ちょっとした準備

- 0 を除いた整数の集合を $\mathbb{Z}^\times$ で表す：　$\mathbb{Z}^\times = \mathbb{Z} - \{0\} = \{\pm 1, \pm 2, \pm 3, \cdots\}$.
- 一般に 2 つのもの A と B について，それらに定数倍と和が定義されているとき，p と q を定数として $pA + qB$ を A **と** B **の線形結合，または 1 次結合** (*linear combination*) と言う．幾何学的 vector で，$s\overrightarrow{\mathrm{a}} + t\overrightarrow{\mathrm{b}}$ はおなじみであろう．線形結合で，scalar 量 p と q がどのような数かが重要である．通常の幾何学的 vector の場合には，$p, q \in \mathbb{R}$ であるから,『実数係数線形結合』と言われる．
- $a, b \in \mathbb{Z}^\times$ について，a と b の**整数係数線形結合** $pa + qb \quad (p, q \in \mathbb{Z})$ の全体を $L(a, b)$ で表す:

$$L(a, b) \overset{\text{def}}{=} \left\{ pa + qb \,\middle|\, p, q \in \mathbb{Z} \right\}.$$

また，値が正であるような $a, b(\in \mathbb{Z})$ の線形結合の全体を $L^+(a, b)$ で表す：

$$L^+(a, b) \overset{\text{def}}{=} \left\{ pa + qb \,\middle|\, p, q \in \mathbb{Z},\ pa + qb > 0 \right\}.$$

次の事実は認めることにする：

Proposition 1.1 (正整数の集合の最小元)
(WO)：正整数 $\mathbb{Z}^+$ の任意の部分集合は，最小元をもつ.

この命題 Proposition 1.1 は，数学的帰納法と同値である．つまり，数学的帰納法が正しいことを認めれば，それから証明できるし，逆にこの命題から数学的帰納法が正しいことが示される．

今後，この命題を $\mathbb{Z}^+$ **の整列性** (*well-orderedness of* $\mathbb{Z}^+$) と呼び，(WO) と略記する．

2　整除性 Divisibility

まず，整数環 $\mathbb{Z}$ は除法をもっていないことに注意しよう．つまり，$\mathbb{Z}$ においては，加減乗法は自由に行えるが，除法はできない．これが，有理数の集合 $\mathbb{Q}$ や実数の集合 $\mathbb{R}$ との大きな違いである．加減乗除，つまり四則が自由にできるような集合を**体 (タイ)**(*field*) と言う．有理数や実数が体であるのに対して $\mathbb{Z}$ は体ではない．

しかし，整数論の核心は，以下で定義される除法，およびそれに付随する剰余 (余り) を巡って展開されてきたし，今後もそうであることは確かである．

本論に入ろう．

Definition 2.1 (整除性)
$a \in \mathbb{Z}^\times$, $b \in \mathbb{Z}$ について，ある $q \in \mathbb{Z}$ が存在して $b = aq$ が成り立つとき，

a は b を割り切る (divide)，a は b の約数である，b は a によって整除される，
b は a の倍数である

と言い，$a \,|\, b$ で表す：

$$a \,|\, b \overset{\text{def}}{\iff} \exists q \in \mathbb{Z} : b = aq.$$

この否定は $a \nmid b$ と表される．

この定義 Definition 2.1 から，次の定理 Theorem 2.2 は直ちに導かれる：

THEOREM 2.2 (除法の諸性質)

$a, b, c \in \mathbb{Z}$ について

(i) $a \,|\, b \Rightarrow \forall k \in \mathbb{Z} : a \,|\, kb.$

(ii) $a \,|\, b \wedge b \,|\, a \Rightarrow a = \pm b.$

(iii) $a \,|\, b \wedge b \,|\, c \Rightarrow a \,|\, c.$

(iv) $a \,|\, b \wedge a \,|\, c \Rightarrow \forall s, t \in \mathbb{Z} : a \,|\, sb + tc.$

(v) $\forall k \in \mathbb{Z}^{\times} : a \,|\, b \iff ka \,|\, kb.$

すべて，整除性の定義からの直接の帰結であるから，証明は省略する．

THEOREM 2.3 (除法の原理 Principle of Division)

$a \in \mathbb{Z}^{\times}$, $b \in \mathbb{Z}$ について，ある整数 q, r がただ 1 つ存在して

$$b = aq + r,\ 0 \leq r < a$$

が成り立つ．

この Theorem 2.3 は，英語では **Division Algorithm** と呼ばれることが多い．直訳すれば「除法の計算手順」である．この定理が，商と余りを求める際の計算法を示していることによるのであろう．しかし以下では除法の原理と呼ぶ．このような基本的・根源的な定理の証明において，$\mathbb{Z}^+$ の整列性 (WO) (Proposition 1.1 (p.2)) が用いられることに着目して欲しい．

Proof.

S を有理数 $\dfrac{b}{a}$ よりも大きい正整数の集合とする：

$$S \overset{\text{def}}{=} \left\{ s \in \mathbb{Z}^+ \,\middle|\, s > \frac{b}{a} \right\}.$$

$\mathbb{Z}^+$ の整列性 (WO) より S は最小元をもつ．それを m とすると

$$m - 1 \leq \frac{b}{a} < m.$$

そこで $q = m - 1$ とすれば $qa \leq b < (q+1)a$ であるから，$r = b - aq$ として

$$b = aq + r,\ 0 \leq r < a.$$

q, r の一意性を示す．b が

$$b = aq + r = aq_1 + r_1,\ 0 \leq r, r_1 < a$$

と 2 通りに表されたとすると，

$$a\,(q - q_1) = r_1 - r, \quad \therefore\ a \,\big|\, r_1 - r.$$

ところが，$-a < r_1 - r < a$ であるから，$r_1 - r = 0$ より $r = r_1,\ q = q_1$ が成り立つ． ■

除法の原理における q を，a を b で割った**商** (*quotient*)，また r を**余り**，**剰余** (*remainder, residue*) と言う．そして，任意に与えられた $a \in \mathbb{Z}^{\times}$, $b \in \mathbb{Z}$ から，商 q と余り r を求める演算を**除法** (*division*) と呼ぶ．

Definition 2.4 (最大公約数 GCD)

$a, b \in \mathbb{Z}^{+}$ を割り切るような，正で最大の整数を「a と b の**最大公約数**」(*the Greatest Common Divisor* GCD) と呼び，それを (a, b) で表す[1]．

次の点に注意されたい：

- $a = b = 0$ ならば，a と b の最大公約数は存在しない．
- $a = 0,\ b \neq 0$ ならば，$(a, b) = (0, b) = \big|b\big|$.
- a, b のいずれも「0 でない」ならば，$\big|a\big| \leq \big|b\big|$ のとき，a の正の約数をすべて列挙して，それらの内で b の約数であるものを探せば，a と b の公約数を得る．その内で最大のものが最大公約数 (a, b) である．

次の定理 Theorem 2.5 によって，a, b と (a, b) の 3 者の関係が鮮明になる．$L^{+}(a, b)$ は，$a, b \in \mathbb{Z}$ の整数係数線形結合 $pa + qb$ の内で, 値が正であるものの全体を表したことを思い出されたい．Section. 1 (p.2) を見よ．

THEOREM 2.5 (最大公約数と線形結合)

$a, b \in \mathbb{Z}^{\times}$ について $(a, b) = d$ とすると，d は a と b の線形結合で表される正整数のうち，最小のものである．つまり

$$(a, b) = \min L^{+}(a, b).$$

Proof.

a と b の整数係数線形結合の集合は，もちろん正の数を含む．そこで $\mathbb{Z}$ の部分集合として $L^{+}(a, b)$ を考えれば，$\mathbb{Z}^{+}$ の整列性 (WO) によって $L^{+}(a, b)$ は最小元をもつ．その最小元を m とする．証明すべきことは $(a, b) = m$ である．

[1] 記号として (a, b) は，a と b の順序対 (点の座標のような) と混同しやすい．そこで，以下では順序対を表す場合には left-angle '⟨' と right-angle '⟩' を用いて，$\langle a, b \rangle$ を用いることにする．

$s, t \in \mathbb{Z}$ によって $m = sa + tb$ と表されたとしよう．a を m で割れば，除法の原理から

$$a = mq + r,\ 0 \leq r < m$$

をみたす $q, r \in \mathbb{Z}$ が存在する．この q, r について

$$r = a - mq = a - (sa + tb)q = (1 - qs)a + (-qt)b$$

であるから，r も a と b の線形結合で表される．

ところが $r < m$ であるから，m の定義より $r = 0$ となり，$a = mq$，つまり $m \mid a$ が成り立つ．

同様にして b についても $m \mid b$ が示されるから，m は a と b に共通する約数である．

d は a と b の最大公約数であるから，d は a と b の任意の線形結合を割り切る．よって $d \mid m$ より $d \leq m$ であるが，d の最大性より $d = m$ が帰結し，定理が成り立つ． ■

この定理 Theorem 2.5 の意味するのは，

#1. a と b の最大公約数は，かならず a と b の線形結合で表される，ということ，つまり $d = (a, b)$ ならば，$d = sa + tb$ をみたす整数 s と t が存在する，ということであり，更に

#2. $d = (a, b)$ は，その線形結合で表される整数 $sa + tb$ の内，正で最小の値に一致する

ということに他ならない．これにより，次の Corollary の証明が容易になる：

Corollary 2.6

$a, b, c \in \mathbb{Z}$ について，$c \mid a \wedge c \mid b \Rightarrow c \mid (a, b)$.

Proof.

Theorem 2.5 によって，ある $s, t \in \mathbb{Z}$ が存在して $d = (a, b) = sa + tb$ であるから，$c \mid d$ が成り立つ． ■

THEOREM 2.7 (最大公約数の性質)

次が成り立つ：

(i) $\forall c \in \mathbb{Z}^+ : (ca, cb) = c(a, b)$.

(ii) $d = (a, b)$ とすれば，$\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = 1$.

Proof.

(i) 2 つの整数 ca, cb の正最小の線形結合の値は，a, b の正最小の線形結合の値の c 倍であることは明らかであり，Theorem 2.5 より (i) は確かに成立する．

(ii) (i) の a を $\dfrac{a}{d}$ に，b を $\dfrac{b}{d}$ に読み替え，c を d とすれば，

$$d\left(\frac{a}{d}, \frac{b}{d}\right) = (a, b) = d, \quad \therefore \left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

が成り立つ．

これで証明された. ■

Definition 2.8 (互いに素)

$a, b \in \mathbb{Z}$ が**互いに素** (*relatively prime, coprime*) であるとは，$(a, b) = 1$ が成り立つことである.

また，k 個の整数 $a_1, a_2, \ldots, a_k$ が**すべて互いに素** (*coprime in pairs*) とは，$i \neq j$ $(1 \leq i, j \leq k)$ なるどの対 $\langle a_i, a_j \rangle$ についても，その最大公約数 $d_{ij} = (a_i, a_j)$ が 1 であることである：

$$\forall i, j : \ i \neq j \ \Rightarrow (a_i, a_j) = 1.$$

例えば 3 個の整数 6, 7, 25 は，$(6, 7) = (6, 25) = (7, 25) = 1$ であるから，すべて互いに素であるが，3 個の整数 6, 14, 25 は $(6, 14) = 2$ であるから,「すべて互いに素である」とは言えない.

一般に k 個の整数がすべて互いに素ならば，それらの数の最大公約数は 1 であるが，逆は言えない. 誤りやすいとことである. 注意して欲しい.

既に証明した Theorem 2.5 (p.4) と，この互いに素であることの定義を結びつけると，極めて重要かつ有用な次の命題を得る：

THEOREM 2.9 (互いに素と線形結合)

$a, b \in \mathbb{Z}$ について，ある $s, t \in \mathbb{Z}$ が存在して $sa + tb = 1$ ならば，a と b は互いに素である. 逆も成り立つ：

$$1 \in L(a, b) \iff (a, b) = 1.$$

---

2 つの整数が互いにあることに関連するいくつかの重要な性質を，定理としてまとめておこう. 特に次の Theorem 2.10 は,『**整数論の基本定理**』(*the Fundamental Theorem of Arithmetic*)(Theorem 3.3 (p.9)) の証明で重要な役目を果たす.

THEOREM 2.10 (Euclid)

$a, b, c \in \mathbb{Z}$ について

$$a \,|\, bc \wedge (a, b) = 1 \ \Rightarrow a \,|\, c.$$

Proof.

Theorem 2.7 (p.5) より $(ac, bc) = c(a, b) = c$ であり，$a \,|\, ac$ は明らかで，更に仮定より $a \,|\, bc$. 従って，a は (ac, bc) を割り切るから，Corollary 2.6 (p.5) より $a \,|\, c$. ■

THEOREM 2.11 (Euclid)

$a, b, c \in \mathbb{Z}$ について，

(i) $(a, b) = (a, c) = 1 \ \Rightarrow (a, bc) = 1.$

(ii) $a \,|\, c \wedge b \,|\, c \wedge (a, b) = 1 \ \Rightarrow ab \,|\, c.$

Proof.

(i) Theorem 2.9 (p.6) より，ある $s, t, u, v \in \mathbb{Z}$ が存在して $sa+tb=1$, $ua+vc=1$ が成り立つ．従って

$$tb \cdot vc = (1-sa)(1-ua) = 1-(s+u-sua)a$$

が成り立ち，$s+u-sua=k$ とすれば $ka+tvbc=1$ であるから，$1 \in L(a, bc)$．つまり a と bc の線形結合が 1 を含むから，再び Theorem 2.9 より a と bc は互いに素である．

(ii) $b \mid c$ より $c=kb$ と置けて，$k \in \mathbb{Z}$ である．$a \mid kb$ であり，かつ $(a, b)=1$ であるから，$a \mid k$. そこで $k=la\,(l \in \mathbb{Z})$ とすれば，$c=lab$ であるから，$ab \mid c$.

これで示された． ■

最大公約数 GCD の双対的な概念としての，

最小公倍数 (*the Least Common Multiple* LCM)

を定義して，その性質の考察に進もう．

Definition 2.12 (最小公倍数)

$a, b \in \mathbb{Z}^{\times}$ の共通な正最小の倍数を，a と b の最小公倍数 (LCM) といい，$[a, b]$ で表す．

また k 個の整数 $a_1, a_2, \ldots, a_k$ についても同様にそれらの最小公倍数を定義し，これを $[a_1, a_2, \ldots, a_k]$ で表す．

THEOREM 2.13 (最小公倍数の性質)

$a, b \in \mathbb{Z}$ について，k を a と b の公倍数とすると，a と b の最小公倍数 $[a, b]$ は k を割り切る．従って a と b の任意の公倍数は，$t \in \mathbb{Z}$ によって $t[a, b]$ と表される．

Proof.

$[a, b]=l$ とする．除法の原理より $k=lq+r$, $0 \leq r < l$ が成り立つ．

$a \mid k$ かつ $a \mid l$ より $a \mid r$ である．同様に $b \mid r$. よって r は a と b の公倍数で，かつ $r<l$. l の最小性より $r=0$ となり，$l \mid k$ が成り立つ． ■

THEOREM 2.14 (GCD と LCM)

$a, b \in \mathbb{Z}^{+}$ について

$$(a, b) \cdot [a, b] = ab.$$

Proof.

$(a, b) = d$ とすれば，ある $s, t \in \mathbb{Z}$ について $d = sa + tb$ である (Theorem 2.5 (p.4))．
$d \mid ab$ より $\dfrac{ab}{d} \in \mathbb{Z}$ である．これを n として，$n = [a, b]$ を示せば十分である．
$n = a \cdot \dfrac{b}{d} = \dfrac{a}{d} \cdot b$ であるから，n は a と b の公倍数である．
k を a と b の任意の正の公倍数とするとき，

$$\frac{k}{n} = k \cdot \frac{d}{ab} = \frac{k(sa + tb)}{ab} = \frac{k}{b}s + \frac{k}{a}t \in \mathbb{Z}.$$

よって $n \mid k$ より $n \leq k$ であるから，$n = [a, b]$. ■

3　素数と素因数分解

Definition 3.1 (素数)

1 より大きい正整数 p が，1 と p 以外に約数をもたないとき，p を**素数** (*prime number*) という．これはまた，p が**真の約数** (*proper divisor*) をもたない，とも言われる．

1 より大きく，素数でない整数を**合成数** (*composite number*) という．1 は素数でも合成数でもない．

Lemma 3.2

$a, b \in \mathbb{Z}$ とする．p が素数であり，かつ $p \mid ab$ ならば，p は a と b の少なくとも一方を割り切る：

$$p : \text{prime} \wedge p \mid ab \Rightarrow p \mid a \vee p \mid b.$$

一般に，$p \mid a_1 a_2 \cdots a_k$ ならば，少なくとも 1 つの a_i について $p \mid a_i$ が成り立つ $(1 \leq i \leq k)$.

Proof.

$p \mid ab$ とする．$p \nmid a$ ならば $(p, a) = 1$ だから，Theorem 2.10 (p.6) により $p \mid b$ である．
$p \mid a_1 a_2 \cdots a_k$ とする．$p \mid a_1$ ならば証明すべきことはない．$p \nmid a_1$ ならば，
$p \mid a_2 a_3 \cdots a_k$ である．$p \mid a_2$ ならば証明は終わる．$p \nmid a_2$ ならば $p \mid a_3 \cdots a_k$．...
これを続ければ，$p \nmid a_1, p \nmid a_2, \cdots, p \nmid a_{k-1}$ ならば $p \mid a_k$ となり，Lemma が成り立つ．
■

いよいよ，

整数論の基本定理　Fundamental Theorem of Arithmetic

と呼ばれる，基本定理の証明が可能になる．そのナカミは，諸君全員が知っていることである．曰く，『どんな整数も素因数分解できる』……「アタリマエ!」と言うことなかれ！

諸君が知っていて，またこれまで行ってきたのは，個々に与えられた整数について，**その整数が**素因数に分解できることであった．整数論の基本定理は違う．たとえ実際にある整数が与えられなかったとしても，整数一般について，任意の整数が素因数分解可能である，という命題である．

経験知から原理的根拠へ，この躍動を諸君は体験しているのだ．
ノーガキはこのくらいにして……

THEOREM 3.3 (整数論の基本定理 FTA)

1 より大きな任意の整数はいくつかの素数の積として表される．この表し方は，素数の順序を無視すれば，一意的に定まる．

Proof.

帰謬法による．いくつか (1 個でもよい) の素数の積で表せない正整数が存在するとして，それらの内の最小のものを m とする．

m は素数ではないから，$1 < r < m$, $1 < s < m$ をみたす $r, s \in \mathbb{Z}^+$ によって，$m = rs$ と表される．

ところが r と s は m より小さいから，r, s は素数の積で表される．よって m もいくつかの素数の積で表されることになるが，これは m の定義に反する．

以上より，素数の積で表せないような整数は存在しない．

次に，素数の積としてある整数を表したときの，表現の一意性を示す．これも帰謬法による．1 より大きな整数で，素数の積に表したとき 2 通りに表されるような整数が存在したとしよう．それらの内で最小のものを n とする．明らかに n は素数ではない．この n が次の 2 通りに表されたとしよう：

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}. \quad (\sharp)$$

ここで $p_1, p_2, \ldots, p_r$ はどの 2 つも異なる素数，$q_1, q_2, \ldots, q_s$ も同様とする．

$p_1 \mid n$ であるから，$p_1 \mid q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$ であり，ある q_i について $p_1 \mid q_i$ が成り立つ．ところが p_1 も q_i も素数であるから，$p_1 = q_i$ が言える．

そこで (♯) の両辺を p_1 で割ると，整数 $\dfrac{n}{p_1}$ が 2 通りに素数の積で表される．ところが $1 < \dfrac{n}{p_1} < n$ であるから，n の最小性に反する．

よって，素数の積による表現の一意性が示された． ■

今後，この定理を **FTA** と呼ぶ．このように，ある整数 n を素数の積の形に分解することを，n の**素因数分解** (*prime factorization*) と言うことは，諸君の知るところであろう．

FTA のおかげで，1 より大きい任意の正整数 n は，$p_1, p_2, \ldots, p_k$ をどの 2 つも異なる素数，また累乗の指数 a_i を正整数として

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

の形に，一意的に表せることが保障される．通常は $p_1 < p_2 < \cdots < p_k$ とする．このような形に n を分解したとき，それを n の**標準分解** (*normal factorization*) という．これは，いくつかのものの積を表す記号 $\prod$ を用いて

$$\prod_{i=1}^{k} p_i^{a_i}, \text{ または単に } \prod p_i^{a_i}$$

と表される.

FTA は，2 つの整数 a，b の最大公約数 (a, b) や最小公倍数 $[a, b]$ の見つけ方も教えてくれる．必要ならば素数の累乗の指数として 0 も認めることにすれば，任意の 2 つの正整数 a と b は同じ素数 $p_1, p_2, \ldots, p_r$ の累乗の積として表現される.

このことを用いて，次の定理を得る：

THEOREM 3.4 (素因数分解と GCD，LCM)

$p_1, p_2, \ldots, p_r$ をすべて異なる素数，また a_i, b_i は非負整数とする (ただし $1 \leq i \leq r$). 正整数 a と b が

$$a = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}, \quad b = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$$

と分解されるとき，$m_i = \min\{a_i, b_i\}$，$M_i = \max\{a_i, b_i\}$ と定めれば，a と b の最大公約数 (a, b)，最小公倍数 $[a, b]$ は

$$(a, b) = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r} = \prod p_i^{m_i},$$
$$[a, b] = p_1^{M_1} p_2^{M_2} \cdots p_r^{M_r} = \prod p_i^{M_i}$$

である.

Theorem 3.4 は，Theorem 2.14 (p.7) の証明を大幅に簡略する．2 つの整数 a と b について

$$\min\{a, b\} + \max\{a, b\} = a + b$$

を用いればそれで終わりである．一般に，次のように言える：

乗法的な問題 — それは除法の原理，GCD と LCM などの概念である — は，**FTA** を用いることによって容易に解決される.

FTA によって，次の有名な定理が証明できる．Euclid の『原論』第 IX 巻の命題 20 である：

THEOREM 3.5 (素数の無限性)

無限に多くの素数が存在する.

Proof.

与えられた有限個の素数から，その内には含まれない異なる新たな素数を作ることができる．以下でこれを示す.

n 個の素数 $p_1, p_2, \ldots, p_n$ が与えられたとしよう．P を

$$P = p_1 p_2 \cdots p_n + 1$$

と定める．**FTA** によって P は素因数をもつ．それを q とする．q は P に一致してもよい．この q は $p_1, p_2, \ldots, p_n$ のいずれとも異なることが，次のように解る.

もし q が $p_1, p_2, \ldots, p_n$ の内のいずれかと一致するならば，q は積 $p_1p_2\cdots p_n$ を割り切り，かつ P を割り切るから，その差 1 を割り切ることになる：$q \mid 1$．しかし，q は素数であるから，これは不合理．よって $p_1, p_2, \ldots, p_n$ 以外の素数が存在することになる．

この操作はいくらでも繰り返すことができるから，定理が成り立つ．　■

次に，標準分解から容易に導くことができる，約数の性質を考えよう．一般に，正整数の集合 $\mathbb{Z}^+$ 上で定義された関数を**整数論的関数** (*arithmetical function*) と言う．

$f(n)$ を整数論的関数とする．$f(n)$ が次の性質をみたすとき，関数 $f(n)$ は**乗法的である** (*multiplicative*) と言う：

$$\forall m, n \in \mathbb{Z}^+ : (n, m) = 1 \Rightarrow f(mn) = f(m) f(n).$$

次の 2 つの関数 $\tau(n), \sigma(n)$ は，代表的な，乗法性をもつ整数論的関数である：

Definition 3.6 (約数の個数と総和)

正整数 n について，n の約数の個数を $\tau(n)$ で，また約数の総和を $\sigma(n)$ で表す．ここで，約数はすべて正のものに限る．

次の定理により，$\tau(n)$ と $\sigma(n)$ の値を求める式が得られる．それはいずれも，n の標準分解によっている：

THEOREM 3.7 (標準分解と約数の個数，総和)

N を 1 より大きな正整数とし，N の標準分解を $N = p_1^{n_1}p_2^{n_2}\cdots p_r^{n_r}$ とする．このとき，

$$\tau(N) = (n_1+1)(n_2+1)\cdots(n_r+1) = \prod (n_i+1),$$
$$\sigma(N) = \frac{p_1^{n_1+1}-1}{p_1-1}\frac{p_2^{n_2+1}-1}{p_2-1}\cdots\frac{p_r^{n_r+1}-1}{p_r-1} = \prod \frac{p_i^{n_i+1}-1}{p_i-1}.$$

Proof.

$d = p_1^{d_1}p_2^{d_2}\ldots p_r^{d_r}$ を n のある正の約数とすると，$1 \le i \le r$ なる任意の i について $d_i \le n_i$ であるから，d_i の選び方は $0, 1, 2, \cdots, n_i-1, n_i$ の n_i+1 通りある．従って，指数の列 $(d_1, d_2, \ldots, d_r)$ の定め方は $(n_1+1)(n_2+1)\cdots(n_r+1)$ 通りあり，このそれぞれと N の約数が 1 対 1 に対応する．よって第 1 式が成立する．

第 2 式を導くために，次の式 S を考える：

$$S = \left(1 + p_1 + p_1^2 + \cdots + p_1^{n_1}\right)\left(1 + p_2 + p_2^2 + \cdots + p_2^{n_2}\right)\cdots\left(1 + p_r + p_r^2 + \cdots + p_r^{n_r}\right).$$

式 S の右辺を展開すると，その各項は，それぞれの i について

$$p_1^{a_1}p_2^{a_2}\ldots p_r^{a_r},\ 0 \le a_i \le n_i$$

という形になる．ところが，展開してできるこれらの項全体の集合は，正整数 N の約数全体の集合に一致する．よって求める $\sigma(N)$ はこの S に等しい．

S の各因子を，等比数列の和と考えれば

$$1 + p_i + p_i^2 + \cdots + p_i^{n_i} = \frac{p_i^{n_i+1} - 1}{p_i - 1}$$

であるから，定理の第 2 式を得る． ■

Corollary 3.8

整数論的関数 $\tau(n), \sigma(n)$ は乗法的である．つまり $(N, M) = 1$ のとき，

$$\tau(NM) = \tau(M)\tau(N), \quad \sigma(MN) = \sigma(M)\sigma(N).$$

Proof.

N と M の標準分解を，それぞれ

$$N = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}, \quad M = q_1^{b_1} q_2^{b_2} \dots q_s^{b_s}$$

とすると，$p_1, p_2, \dots, p_r, q_1, q_2, \dots, q_s$ はすべて異なる素数であるから，明らか． ■

4　Euclid の算法

任意に与えられた 2 つの整数 a，b について，その最大公約数 (a, b) を求める計算手順——これを**アルゴリズム　algorithm** という——として**ユークリッドの互除法**，**ユークリッド算法** (*Euclidean Algorithm*) がある．ユークリッドの『原論』第 7 巻命題 2 に

> 与えられた互いに素ではない 2 つの整数についてその最大公約数を求めること
> Δύο ἀριθμῶν δοθέντων μὴ πρώτων πρὸς ἀλλήλους τὸ μέγιστον αὐτῶν κοινὸν μέτρον εὑρεῖν.

という節があり，そこでこの計算手順が説明されている．

『原論』のこの箇所が最も古い記述であろうが，おそらくユークリッド以前に発見されていたものと考えられている．この計算手法は，通常日本語では,『ユークリッドの互除法』と呼ばれるが，元々は *Euclidean Algorithm* であり,「除法」を意味している訳ではない．これ以降，**Euclid 算法**と呼ぶ．またこれを **EA** と略すこともある．

次の補題が，**EA** の核心である：

Lemma 4.1

2 整数 a と b は「どちらも 0」であることはないとする．任意の整数 k について次が成り立つ：

$$(a, b) = (b, a - kb).$$

Proof.

$(a, b) = d$, $(b, a - kb) = \delta$ とする．以下，$d \mid \delta$ かつ $\delta \mid d$ を示す．

I. $d \mid \delta$ が成り立つこと：$(a, b) = d$ であるから，$d \mid b$. また，d は a，b の任意の整係数線形結合を割り切るから $d \mid a - kb$. (Theorem 2.2 (p.3) (iv)) Corollary 2.6 (p.5) より $d \mid (b, a - kb)$，つまり $d \mid \delta$.

II. $\delta \mid d$ が成り立つこと：$(b, a - kb) = \delta$ より $\delta \mid b$. また $a = (a - kb) + kb$ より a は $a - kb$ と b の線形結合であり，I. の場合と同様に $\delta \mid a$. よって $\delta \mid d$.

I, II より $d = \pm\delta$ (Theorem 2.2 (p.3) (ii)) となり，d も δ も正として $d = \delta$. ■

この補題 Lemma 4.1 (p.12) により，与えられた 2 つの整数 a と b の最大公約数 (a, b) を求めるための，

Euclid 算法　Euclidean Algorithm, EA

を得る．まずは，それがどのような algorithm であるかを示す．

$a, b \in \mathbb{Z}$ とする．a, b の一方が 0 のときは他方も 0 ならば最大公約数を考えることは出来ない．すべての 0 でない整数が公約数になる．

他方が 0 でない場合，つまり $\mathbb{Z}^\times$ の要素であるならば，その絶対値が最大公約数になる．つまり任意の $n \in \mathbb{Z}^\times$ について

$$(n, 0) = |n|$$

である．

a, b のいずれも 0 でない場合には，最大公約数を考える場合に正の約数に限定して一般性を失うことはないから，最初から $a, b \in \mathbb{Z}^+$ として考察すれば十分である．このもとで，次の計算手順を考える：

Euclidean Algorithm　(EA)

$\max\{a, b\} = a_1$, $\min\{a, b\} = b_1$ とする．a_1, b_1 から出発して割り算を反復し，その余りを順に $r_1, r_2, \ldots, r_n, \ldots$ とする．つまり，

$$\begin{aligned}
a_1 &= b_1 q_1 + r_1, & r_1 &= a_1 - b_1 q_1, && \text{(step 1)}\\
b_1 &= r_1 q_2 + r_2, & r_2 &= b_1 - r_1 q_2, && \text{(step 2)}\\
r_1 &= r_2 q_3 + r_3, & r_3 &= r_1 - r_2 q_3, && \text{(step 3)}\\
&\cdots & &\cdots &&\\
r_{k-3} &= r_{k-2} q_{k-1} + r_{k-1}, & r_{k-1} &= r_{k-3} - r_{k-2} q_{k-1}, && \text{(step } k-1\text{)}\\
r_{k-2} &= r_{k-1} q_k + r_k, & r_k &= r_{k-2} - r_{k-1} q_k, && \text{(step } k\text{)}
\end{aligned}$$

このとき，

$$a_1 > b_1 > r_1 > r_2 > \cdots > r_{k-2} > r_{k-1} > r_k$$

であるから，非負整数 $\mathbb{N}$ の要素からなる強意の単調減少列ができる．ところが $\mathbb{N}$ **には強意 (狭義) に単調減少する無限列は存在しない**から，この列はどこかで 0 となる．それを r_k としよう：$r_k = 0$.

Lemma 4.1 (p.12) により，

$$(a_1, b_1) = (b_1, r_1) = (r_1, r_2) = \cdots = (r_{k-2}, r_{k-1}) \tag{1}$$

が言える．ところが

$$r_{k-2} = r_{k-1}q_k + r_k = r_{k-1}q_k \qquad \because\ r_k = 0$$

であるから，r_{k-1} は r_{k-2} の約数，つまり $r_{k-1} \,|\, r_{k-2}$ が成り立つ．よって

$$(r_{k-2},\, r_{k-1}) = r_{k-1}$$

となり，(1) と合わせて

$$(a,\, b) = (a_1,\, b_1) = r_{k-1}$$

であることが解る．

定理としておこう：

THEOREM 4.2 (Euclidean Algorithm (EA))

$a, b \in \mathbb{Z}^+$ について，(step 1) から (step k) までの割り算を実行するとき，余りが 0 になる ($r_k = 0$) 直前の余り r_{k-1} が a と b の最大公約数 (a, b) になる．

Euclidean Algorithm は，このようにして与えられた任意の 2 整数 a と b の最大公約数を求める計算手順を与えてくれるが，計算手順そのものとしてよりもむしろ，次の定理 Theorem 4.3 (p.14) を帰結することにこそ，その重要性がある：

THEOREM 4.3 (最大公約数の線形性)

$a, b \in \mathbb{Z}$ について，その最大公約数 (a, b) は，a と b の整係数線形結合で表される：

$$\exists n, m \in \mathbb{Z}:\ (a, b) = na + mb.$$

さらにその最小性により，次のように言える：

$$(a, b) = \min L^+(a, b).$$

Proof.

Euclidean Algorithm で生じる整数列

$$a_1, b_1, r_1, r_2, \ldots, r_N, \ldots \qquad (\sharp)$$

の任意の項が a と b の整係数線形結合で表されることを示せば十分である．一般性を失うことなく $a \geq b$ とできるから，$a = a_1 = r_{-1}$, $b = b_1 = r_0$ として，数学的帰納法による．

(I) Base. $k = -1, 0$ のとき，

$$a_1 = a \cdot 1 + b \cdot 0,\ b_1 = a \cdot 0 + b \cdot 1$$

であるから，明らか．

(II) IS. $k = N,\, N+1$ で成立を仮定する．つまり $\alpha_1,\, \alpha_2,\, \beta_1,\, \beta_2 \in \mathbb{Z}$ として

$$r_N = \alpha_1 a + \beta_1 b, \quad r_{N+1} = \alpha_2 a + \beta_2 b. \tag{IH}$$

$k = N+2$ のとき，r_{N+2} は r_N を r_{N+1} で割った余りだから，商を q として $r_N = r_{N+1}q + r_{N+2}$．従って

$$\begin{aligned} r_{N+2} &= r_N - r_{N+1}q \\ &= (\alpha_1 a + \beta_1 b) - (\alpha_2 a + \beta_2 b)\, q \quad (\because \text{IH}) \\ &= (\alpha_1 - \alpha_2 q)\, a + (\beta_1 - \beta_2 q)\, b. \end{aligned}$$

ここで $\alpha_1 - \alpha_2 q,\ \beta_1 - \beta_2 q \in \mathbb{Z}$ であるから，r_{N+2} も a と b の整係数線形結合で表される．

(I) と (II) により，整数列 (♯) の任意の項は a と b の整係数線形結合で表される．　■

5　1 次不定方程式

一般に，m 変数の方程式が n 本あるとき，$m > n$ ならば解が一意的に定まる訳ではない．こうした方程式を**不定方程式** (*indefinite equation, indeterminate eq.*) と言う．

不定方程式の体系的な考察は，紀元 250 年頃アレクサンドリアで活躍したディオファントス (Diophantus of Alexandria) に始まる．彼は 6 巻からなる『数論』(APIΘMHTIKA, *Arithmetica*) を残している．この数学者の名にちなんで，不定方程式は**ディオファントス方程式** (*Diophantine Equation*) とも呼ばれる．

ディオファントス自身は，不定方程式の有理数解を研究しているが，今日では「ディオファントス方程式論」と言う場合には，不定方程式の整数解の考察を指すのが普通である．

この Section 5 では，特に 2 変数 1 次の，整数係数不定方程式

$$ax + by = c,\ a, b, c \in \mathbb{Z}$$

とその整数解について考察しよう．というのも，この方程式の整数解の存在，及び存在する場合の解の性質は，この Part 1 でのこれまでの我々の考察に深く関わっているからである．

例えば，$2x - 3y = 1$ は，整数係数の不定方程式であり，$\langle x,\, y\rangle = \langle 5,\, 3\rangle$ はこの方程式をみたすから，解である．このような解 1 つ 1 つを，この方程式の**特殊解** (*particular solution*) と言う．特殊解 $\langle 5,\, 3\rangle$ について，方程式に代入した $2\cdot 5 - 3\cdot 3 = 1$ が成り立つから，方程式 $2x - 3y = 1$ からこれを辺々引いて

$$2(x-5) - 3(y-3) = 0 \iff 2(x-5) = 3(y-3)$$

を得る．$(2,\, 3) = 1$ であるから，$x-5$ は 3 の倍数，$y-3$ は 2 の倍数となり，$k \in \mathbb{Z}$ として

$$x - 5 = 3k,\ y - 3 = 2k \iff \begin{cases} x = 5 + 3k, \\ y = 3 + 2k \end{cases}$$

を得る．次の定理 Theorem 5.1 で明らかにされることだが，方程式 $2x-3y=1$ の解は，すべてこの形で表され，これ以外の解は存在しない．そこで，この形の解，つまり $\langle x,\, y\rangle = \langle 5+3k,\, 3+2k\rangle$ $(k \in \mathbb{Z})$ を，この方程式の**一般解** (*general solution*) と言う．

以下,「方程式 $ax+by=c$」と言った場合には，整数係数であるとする．つまり $a,\, b,\, c \in \mathbb{Z}$ であることをいちいち断わらない．また,「$\mathbb{Z}$ 上の方程式 $ax+by=c$」と言うこともある．

THEOREM 5.1 (解の存在条件)

次が成り立つ：

(1) $\mathbb{Z}$ 上の方程式 $ax+by=c$ が整数解をもつための必要十分条件は，$(a,\, b) \,\big|\, c$ である．

(2) $(a,\, b)=d$ とする．この方程式が特殊解 $\langle x,\, y\rangle = \langle X,\, Y\rangle$ をもつならば，$t \in \mathbb{Z}$ として

$$x = X + t\frac{b}{d}, \quad y = Y - t\frac{a}{d} \tag{\#}$$

が一般解であり，またこの方程式の解は (#) に限られる．

Proof.

(i) 方程式 $ax+by=c$ が特殊解 $\langle x,\, y\rangle = \langle X,\, Y\rangle$ $(X,\, Y \in \mathbb{Z})$ をもつとすると $aX+bY=c$ が成り立つ．この左辺は a と b の線形結合であるから，$(a,\, b)=d$ で割り切られる．よって $d \,\big|\, c$ が必要である．

逆に $d \,\big|\, c$ とすれば，$k \in \mathbb{Z}$ として $c=kd$ と置ける．Theorem 2.5 (p.4) によって $d=ra+sb$ $(r,\, s \in \mathbb{Z})$ となる r と s が存在する．そこで $X=kr$, $Y=ks$ として

$$akr+bks=kd \iff aX+bY=c$$

より，$\langle x,\, y\rangle = \langle X,\, Y\rangle = \langle kr,\, ks\rangle$ を解にもつ．

(ii) 次に，一般解についての証明に移る．$\langle X,\, Y\rangle$ が (#) の形のとき，方程式 $ax+by=c$ の左辺にこれを代入すれば

$$\begin{aligned} a\left(X+t\frac{b}{d}\right)+b\left(Y-t\frac{a}{d}\right) &= aX+bY+t\frac{ab-ba}{d} \\ &= aX+bY=c \end{aligned}$$

であるから，任意の $t \in \mathbb{Z}$ について，確かに (#) は $ax+by=c$ の解になる．

逆に $\langle x,\, y\rangle$ が $\langle X,\, Y\rangle$ 以外の，方程式 $ax+by=c$ の解であったとすると

$$ax+by=aX+bY \iff a(x-X)=b(Y-y). \tag{$*$}$$

$(a,\, b)=d$ について $a=d\alpha$, $b=d\beta$ とすれば $(\alpha,\, \beta)=1$ であり ($\because$ Theorem 2.7 (p.5) (ii))，Theorem 2.10 (p.6) によって

$$\beta \,\big|\, x-X, \quad \alpha \,\big|\, Y-y.$$

よって $t \in \mathbb{Z}$ として

$$x - X = \beta t \iff x = X + \beta t = X + t\frac{b}{d}.$$

また $\alpha\beta t = \beta(Y - y)$ より

$$Y - y = \alpha t \iff y = Y - \alpha t = Y - t\frac{a}{d}.$$

以上より，$\mathbb{Z}$ 上の方程式 $ax + by = c$ の解は $(\#)$ の形に限ることが示された．　■

xy 座標平面上の点で，x, y 座標がいずれも整数であるような点を **(整数) 格子点** (*lattice point*) と呼ばれることは，ご存知であろう．2 次元の格子点全体の集合を $\mathbb{Z}^2$ で表す．

上の定理 Theorem 5.1 は，直線 $\ell : ax + by = c$ $(a, b, c \in \mathbb{Z})$ が 1 つの格子点を通るならば，ℓ は無限個の格子点を通ることを述べている．つまり，a, b, $c \in \mathbb{Z}$ について $L = \left\{ \langle x, y \rangle \in \mathbb{Z}^2 \,\middle|\, ax + by = c \right\}$ とすれば，

$$L \neq \emptyset \Rightarrow L \text{は無限集合}$$

ということに他ならない．

最後に，$\mathbb{Z}$ 上の方程式 $ax + by = c$ が正の解 $\langle x, y \rangle \in \mathbb{Z}^+ \times \mathbb{Z}^+$ をもつための，a, b, c についての条件に関する定理を示そう．

係数 a と b について，$(a, b) = 1$ として一般性を失わない．なぜなら，$ax + by = c$ が解をもつ以上，Theorem 5.1 (p.16) より，c は $(a, b) = d$ の倍数であるから，両辺を d で割って

$$a_1 x + b_1 y = c_1, \quad (a_1, b_1) = 1,\ c_1 = \frac{c}{d} \in \mathbb{Z}$$

となるからである．

次の定理が成り立つ：

THEOREM 5.2 (正の整数解)

$a, b, c \in \mathbb{Z}^+$, $(a, b) = 1$ とし，X, Y を $ax + by = c$ の特殊解とする．

このとき，$ax + by = c$ の正整数解の個数は，$-\dfrac{X}{b} < t < \dfrac{Y}{a}$ をみたす $t \in \mathbb{Z}$ の個数に一致する．

特に $c > nab$ ならば，$ax + by = c$ は少なくとも n 個の正整数解をもつ．

Proof.

一般解 $x = X + t\dfrac{b}{d}$, $y = Y - t\dfrac{a}{d}$ で，$d = 1$ であり，このいずれも正であるから

$$\begin{cases} x = X + tb > 0, \\ y = Y - ta > 0 \end{cases} \iff t > -\frac{X}{b},\ t < \frac{Y}{a} \iff -\frac{X}{b} < t < \frac{Y}{a}.$$

これをみたす $t \in \mathbb{Z}$ ごとに正の解 $\langle x, y \rangle$ が定まるから，定理の前半が成り立つ．

したがって，もし $\dfrac{Y}{a}-\dfrac{-X}{b}>n$ であれば，$ax+by=c$ は少なくとも n 個の解をもつが，

$$\frac{Y}{a}-\frac{-X}{b}>n \iff aX+bY>nab$$

であることと，$aX+bY=c$ であることから，$c>nab$ となり，後半も成り立つ． ■

以上で，整数論の最基底にある領域に関する考察を終える．続く

MJK New Series, No.Z02. 整数論の基礎 Part 2. 剰余と合同関係

では，かの大ガウスに始まる合同式の本格的考察に踏み込むことにしよう．

(to be continued to Part 2.)