プログラミングの背景：数論

記号と準備

tbasic.org [*1]

[2017 年 6 月版]

数学的な内容を正確に述べようとするとき，必ずそのための前提となる事柄についての了解が必要です。かなり厳格な扱いをする場合は，公理からの記述となるでしょう。勿論，ここではそのような厳格な扱いをするわけではありません。しかし，説明の根拠となる前提の内容について確認をすることは重要なことです。そしてそれを起点として，説明や証明するという姿勢は大切なことと考えます。

ここでは，"プログラミングの背景：数論" での説明や証明に使われる記号や数学的基本性質についてまとめます。勿論完璧なものではありません。日常的に普通に使われている記号や事柄については特に説明しなくて使用することも，多々あります。

この文書は必要に応じて随時更新します。

目次

[*1] http://www.tbasic.org

1 記号と用語

ここでは，「プログラミングの背景」で使われる基本的な記号や用語の定義や説明を簡単にまとめます。ここでは，これらの性質の説明というより，既にここに述べられている内容を何らかの形で知っている人のための再確認のためのものです。

1.1 論理

ここでは，論理に関する記号や用語の最小限の確認します。

命題と真理値

- 真偽の定まる主張（又は真偽が定まっていると考える主張）を**命題**（proposition）或は言明（statememt）という。命題の真偽を**真理値**（truth value）と言う。真をT（True），偽をF（False）で表す。

論理記号 p, q を命題とする。

- 命題「p でない」("not p"）を $\neg p$ と表す。
- 命題「p かつ q」("p and q"）を $p \wedge q$ と表す。
- 命題「p または q」("p or q"）を $p \vee q$ と表す。
- 命題「p ならば q」("if p, then q"）を $\mathrm{p} \Rightarrow q$ と表す。
- 命題「p と p は同値」("p is equivalent to q"）を $p \Leftrightarrow q$ と表す。

述語

- x があるものの中を動くとき，各 x_0 に対して，$p(x_0)$ が命題となるとき，$p(x)$ を（1 変数）述語という。同様に，多変数述語 $q(x, y, \ldots)$ が定義される。

述語論理記号 $p(x)$ を述語とする。

- 述語「すべての x について $p(x)$ である」("for all x, $p(x)$"）を $\forall x p(x)$ または，$\forall x(p(x))$ と表す。
- 述語「ある x について $p(x)$ である」,「$p(x)$ となる x が存在する」　("for some x , $p(x)$"）を $\exists x p(x)$ または，$\exists x(p(x))$ と表す。また，$\exists x$ s.t. $p(x)$ と表すこともある[*2]。

1.2 集合

ここでは，集合に関する記号や用語の最小限の確認します。

- A を集合とするとき，a が 集合 A の元（要素）であることを $a \in A$ と表す。元でないことを $a \notin A$ と表す。
- A, B を集合とする。A の元がすべて B の元でもあるとき，A は B の**部分集合**であると言って，$A \subset B$ または，$B \supset A$ と表す。

[*2] ここでの，"s.t." は "such that" の略号で，"there exisit x such that $p(x)$" を意味します。

- $a, b, c, \cdots$ をあるものとする。$a, b, c, \cdots$ のみを元とする集合を $\{a, b, c, \cdots\}$ と表す。

（集合の外延的定義）

- A を集合とする。$p(x)$ を A の元 x の性質とする。このとき，A の元 a で $p(a)$ となる全体からなる A の部分集合を $\{a \in A \mid p(a)\}$ と表す。

（集合の内包的定義）

- $\mathcal{U}$ を集合とし，この $\mathcal{U}$ を固定し，常に $\mathcal{U}$ の部分集合のみを考えるとき，$\mathcal{U}$ を**全体集合**という。全体集合が良く分かっているとき，$\{x \in \mathcal{U} \mid p(x)\}$ の替わりに $\{x \mid p(x)\}$ と表すこともある。
- 元を全く含まないものも集合と考える。これを**空集合**といって，$\emptyset$ と表す。即ち $\emptyset$ は，$\forall x(x \notin \emptyset)$ が真になるもの。

集合の基本的演算

A，B を集合とする。

- A の元と B の元をすべて集めてできる集合を，A と B の**和集合**と言って，$A \cup B$ と表す。即ち，$A \cup B$ は

$$(x \in A \cup B) \Leftrightarrow ((x \in A) \vee (x \in B))$$

で特徴付けられる。このことから，$A \cup B = \{x \mid (x \in A) \vee (x \in B)\}$ と表すこともある。
- 集合 A と B に共に含まれる元をすべて集めてできる集合を，A と B の**共通部分（共通集合）**と言って，$A \cap B$ と表す。即ち，$A \cap B$ は

$$(x \in A \cap B) \Leftrightarrow ((x \in A) \wedge (x \in B))$$

で特徴付けられる。このことから，$A \cap B = \{x \mid (x \in A) \wedge (x \in B)\}$ と表すこともある。
- $A \cap B = \emptyset$ のとき，A と B は互いに素な集合であるという。
- B 含まれない A の元をすべて集めてできる集合を，A から B を引いた**差集合**と言って，$A - B$ と表す。即ち，$A - B$ は

$$(x \in A - B) \Leftrightarrow ((x \in A) \wedge (x \notin B))$$

で特徴付けられる。このことから，$A - B = \{x \mid (x \in A) \wedge (x \notin B)\}$ と表すこともある。
- 全体集合 $\mathcal{U}$ が定められているとき，$\mathcal{U} - A$ を A の補集合と言って，A^c と表す。即ち，A^c は

$$x \in A^c \Leftrightarrow x \in \mathcal{U} - A \Leftrightarrow (x \in \mathcal{U}) \wedge (x \notin A)$$

で特徴付られる。これから，$A^c = \{x \in \mathcal{U} \mid x \notin A\} = \{x \mid x \notin A\}$ と表すこともできる[*3]。

1.3 数の集合

- $\mathbb{N}$：自然数すべてのなす集合，即ち，$\mathbb{N} = \{1, 2, 3, \cdots\}$ である[*4]。
- $\mathbb{Z}$：整数すべてのなす集合，即ち，$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \cdots\}$ である。
- $\mathbb{R}$：実数すべてのなす集合。
- $\mathbb{C}$：複素数すべてのなす集合。

[*3] 補集合の記法を用いたときは，特に説明しなくても全体集合が定められているとします。
[*4] 0 を自然数とする立場もありますが，ここでは自然数は 1 から始めることにします。

- 数の集合について， $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{R} \subset \mathbb{C}$ となる。
- a を実数とするとき，

$$|a| = \begin{cases} a & ; a \geqq 0 \text{ のとき} \\ -a & ; a < 0 \text{ のとき} \end{cases}$$

  と定義して， $|a|$ を a の**絶対値**という。
- A を実数の部分集合とする。A の元 a_0 で，A の任意の元 a に対して，$a_0 \leqq a$ となるものが存在するとき，a_0 を A の**最小元**と言って，$\min(A)$ と表す。
  同様に，A の元 a_1 で，A の任意の元 a に対して，$a_1 \geqq a$ となるものが存在するとき，a_1 を A の**最大元**と言って，$\max(A)$ と表す。
- A を実数の部分集合とする。$M \in \mathbb{R}$ が A の**上界**とは，

$$A \text{ すべてのの元 } x \text{ に対して}, x \leqq M \text{ となる。}$$

  ことを言う。上界が存在するとき，**上に有界**であると言う。同様に，$m \in \mathbb{R}$ が A の**下界**とは，

$$A \text{ のすべての元 } x \text{ に対して}, m \leqq x \text{ となる。}$$

  ことを言う。下界が存在するとき，**下に有界**であると言う。上にも下にも有界であるとき，単に**有界**であると言う。
- 自然数の部分集合は常に下に有界である。

2　基本的概念と性質

ここでは，前節と異なり，確認の意味もありますが，内容の補足を含めての多少の説明をします。勿論ここでの記述が，ここに述べている事項の自習用テキストを目的としているわけではありませんので，十分な内容ではありません。

2.1　数学的帰納法

自然数，あるいはその拡張型である整数は身近で，ある意味分かりやすい対象と言えます。しかし，それらは私たちが最初に出会った無限の対象で，その持っている性質は私たちの想像をはるかに超える広さと深さを持っています。それゆえに，その内容の正確な理解を得るには，特に無限的性質については正確な理解を得るためには，慎重に論法を進める必要があります。

古くから，自然数での無限的性質の証明のために，その原理・方法が考えられてきました。古代ギリシアでは，「原論」に見られるように，数学的体系の考察が深くなされ，公理，公準からの証明という数学的体系が構成されていました。しかし，それらに含まれる個々の証明の中身は，正しいものであるものの，幾分直感的なものから構成されていました。

中世，ルネッサンス時期になると，自然数について深い形式的結果が得られるようになり，その証明方法として数学的帰納法的な手法が用いられるようになりました。しかし，現在私たちが使っている数学的帰納法について明確に認識し，形式化されたのは近世に入ってからで，デデキント（1831-1916）やペアノ（1858-1932）らによって成されました。

数学的帰納法は自然数の無限に関する性質を規定する原理です。その意味で，自然数，そしてその拡張型である整数での性質の証明は突き詰めれば，すべて数学的帰納法に依拠していると言えます。このことから，数学的帰納法は次の２つの意味で重要なものと言えます。

- 数学的帰納法は自然数の構造の本質を示す。
- 種々の性質の証明の基本的道具である。

数学的帰納法は，高校の教科書にも載っているものですが，ここでは，数学的帰納法の基本的内容の確認をしましょう。

数学的帰納法は次の形でよく用いられます。

数学的帰納法 1

$P(n)$ を自然数 n についての主張とし，次の性質 (1) と (2) を満たすとする。

(1) $P(1)$ が成立

(2) 全ての自然数 n に対して，次が成立する。

"$P(n)$ が成立すれば，$P(n+1)$ も成立する。"

このとき，任意の自然数 n に対して $P(n)$ が成立する。

この形の数学的帰納法は，高校の教科書にもあり，その例もよく見られるものですので，ここでは 1 つ例をあげるだけにします。

例 2.1.

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = (1 + 2 + 3 + \cdots + n)^2 \tag{$*$}$$

証明 今の場合，$P(n)$ は，上の等式 $(*)$ がすべての自然数 n に対して成立するという主張になる。

(1) $n = 1$ のときは，$1^3 = 1^2$ なので成立する。

(2) n のとき，主張が成立と仮定する。[*5]。即ち，

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = (1 + 2 + 3 + \cdots + n)^2 \tag{1}$$

が成立すると仮定する。さて，右辺の式を n の代わりに $n + 1$ とした式を考える。それを展開すると，

$$(1 + 2 + 3 + \cdots + n + (n + 1))^2 = (1 + 2 + 3 + \cdots + n)^2 + 2((1 + 2 + 3 + \cdots + n)(n + 1) + (n + 1)^2 \tag{2}$$

と変形できる。ここで，よく知られた等差級数の和の公式

$$1 + 2 + 3 + \cdots + n = \frac{n(n + 1)}{2} \tag{3}$$

に注目する[*6]。この式 (3) を上の式 (2) 右辺の第 2 項に代入すると次が得られる。

$$\begin{aligned} (1 + 2 + 3 + \cdots + n + (n + 1))^2 &= (1 + 2 + 3 + \cdots + n)^2 + n(n + 1)^2 + (n + 1)^2 \\ &= (1 + 2 + 3 + \cdots + n)^2 + (n + 1)(n + 1)^2 \\ &= (1 + 2 + 3 + \cdots + n)^2 + (n + 1)^3 \end{aligned} \tag{4}$$

この式 (4) の最後の右辺の第 1 項に，帰納法の仮定 (1) を代入すると，次が得られる。

$$(1 + 2 + 3 + \cdots + n + (n + 1))^2 = 1^3 + 2^3 + 3^3 + \cdots + n^3 + (n + 1)^3$$

この式は $n + 1$ のときの示すべき式だった。即ち，$n + 1$ のときも，主張は成立する。

以上の (1),(2) の結果から数学的帰納法により，すべての自然数 n に対して，主張 $(*)$ が成立することが示された。 □

[*5] これを帰納法の仮定と言います。

[*6] この式は数学的帰納法で証明する例として有名です。

数学的帰納法はもう一つ別の次の形（数学的帰納法 2）で利用されることもあります。

数学的帰納法 2

$P(n)$ を自然数 n についての主張とし，次の性質 (1) と (2) を満たすとする。

(1) $P(1)$ が成立

(2) 全ての自然数 n に対して，次が成立する。

"$P(1),\ldots,P(n)$ が成立すれば， $P(n+1)$ も成立する。"

このとき，任意の自然数 n に対して $P(n)$ が成立する。

数学的帰納法 2 では，(2) の前提条件が少し強くなっていますが，この形でも上のものと同値であることが示されます。

２つの数学的帰納法の同値性

数学的帰納法 1 と数学的帰納法 2 は同値である。

即ち，数学的帰納法 1 が成立すると仮定すると，数学的帰納法 2 が証明され，逆に数学的帰納法 2 が成立すると仮定すると，数学的帰納法 1 が証明される。

証明 [*7]

[$\Longrightarrow$] 数学的帰納法 1 が成立すると仮定する。このとき，数学的帰納法 2 が成立することを数学的帰納法 1 を使って証明する。まず，数学的帰納法 2 を少し変更した数学的帰納法 2' を考える。

数学的帰納法 2'

$P(n)$ を自然数 n についての主張とし，次の性質 (1) と (2) を満たすとする。

(1) $P(1)$ が成立

(2) 全ての自然数 n に対して，次が成立する。

"$P(1),\ldots,P(n)$ が成立すれば， $P(n+1)$ も成立する。"

このとき，任意の自然数 n に対して，$P(1),\ldots,P(n)$ が成立する。

数学的帰納法 2' は数学的帰納法 2 より，強い主張だから，数学的帰納法 2' を示せばよい[*8] 。

(1) $n=1$ のとき，条件 (1) より，$P(1)$ は成立する。

(2) n について主張が成立と仮定する。即ち，「$P(1),\ldots,P(n)$ が成立」とする。このとき，条件 (2) より，$P(n+1)$ が成立する。一方帰納法の仮定から $P(1),\ldots,P(n)$ も成立する。即ち，$P(1),\ldots,P(n),P(n+1)$ が成立する。これは $n+1$ のときの主張に他ならない。故に数学的帰納法 2' の成立が示された。従って，数学的帰納法 2 も成立する。

[*7] 以下は証明法についての証明で，幾分デリケートです。注意深くお読みください。

[*8] 数学的帰納法 2' は数学的帰納法 2 の結論を n 以下の自然数にも成立するとしたのもので，形式的には，強い主張ですが，最終的にはすべての自然数 n について成立するという結論ですから，結局，主張は同じで，むしろ冗長な表現です。

[⟸] 数学的帰納法 2 が成立すると仮定する。このとき，数学的帰納法 1 が成立することを示す。数学的帰納法 1 の前提 (2) の前提は「$P(n)$ が成立」である。他方，数学的帰納法 2 の前提 (2) の前提は「$P(1),\dots,P(n)$ が成立」である。数学的帰納法 1 では前提 (2) が「$P(n)$ が成立」という前提で示されるので，それを含んだ多くの「$P(1),\dots,P(n)$ が成立」からは勿論示される。従って， 数学的帰納法 2 の結論が得られる。数学的帰納法 1 の結論は数学的帰納法 2 の結論と同じだから，数学的帰納法 1 の結論が得られ，数学的帰納法 1 が成立することが得られた。 □

数学帰納法 2 の形の方が (2) の前提条件が少し強い分[*9]，証明に使う際には強力です。そのことから，少し込み入った実際の数学では数学帰納法 2 の方が，使われることが多いようです。

この数学的帰納法 2 の適用の例を 2 つあげましょう。ただ，以下の証明は少し難解かもしれません。そこで，より直感的な説明もあげました。この説明で納得できれば，証明は飛ばしても良いかもしれません。

次は自然数についての重要な性質です。

自然数の整列性

A を $\mathbb{N}$ の空でない部分集合とすると，A には最小元が存在する。

説明 $1,2,3,\dots$ と順に A の元であるかどうか確認し，最初に A の元になったものが，最小元です。A は空でないので，いずれ A の元になるものが現れます。 □

証明 A に最小元が存在しないと仮定する。このとき，数学的帰納法を用いて

すべての $n\in\mathbb{N}$ 対して，$n\notin A$ となる

ことを示す。今の場合， $P(n)$ は，”$n\notin A$” になる。

(1) $1\in A$ なら，1 は A の最少元になるから，仮定に反する。従って，$1\notin A$ となる。

(2) ある自然数 n_0 に対して，数学的帰納法 2 の (2) 条件が成立しないとする。即ち，$P(1),\dots,P(n_0)$ は成立するが，$P(n_0+1)$ は成立しないとする。これは，$1\notin A,\dots,n_0\notin A$ で，$n_0+1\in A$ を意味している。しかし，これは，n_0+1 が A の最小元であると主張している。これは仮定に反する。従って，このような n_0 は存在しない。即ち，数学的帰納法 2 の (2) 条件はすべての自然数 n に対して成立する。

以上から，主張 $P(n)$ はすべての自然数 n に対して成立する。従って，A は空集合になる。これは A が空集合でないという前提に反する。従って，A に最小元が存在しないと仮定は矛盾，即ち，A には最小元が存在する。 □

次の性質も $\mathbb{N}$ の重要な性質です。明らかな感じもする性質ですが，数学的帰納法で証明しましょう。

$\mathbb{N}$ の有界集合での最大値の存在性

B を $\mathbb{N}$ の有界な空でない部分集合とすると，B には最大元が存在する。

[*9] 従って (2) の全体は弱い条件になります。

説明 B は自然数の部分集合で有界なので，有限集合になります。従って，それら有限個の元の中で一番大きいものが最大元になります。 □

証明 $\bar{B}$ を B のある元以下の自然数の全体，即ち

$$\bar{B} = \{n \in \mathbb{N} \mid \exists x \in B \ \ s.t. \ \ n \leqq x\}$$

とする。このとき，$\bar{B}$ も有界になる。実際 B の上界は $\bar{B}$ の上界にもなる。

更に，$\bar{B}$ の最大元 $b_0 = \max \bar{B}$ が存在すれば，それは B の最大元にもなる。実際，$b_0 \in \bar{B}$ だから，$b_0 \leqq b_1$ となる $b_1 \in B$ が存在する。しかし，$b_1 \in \bar{B}$ だから，$b_0 = \max \bar{B}$ より，$b_1 \leqq b_0$ となり，即ち，$b_0 = b_1 \in B$ が得られる。従って，$b_0 = \max B$ になる。

そこで，$\bar{B}$ に最大元が存在しないと仮定する。このとき，数学的帰納法を用いて

$$\text{すべての } n \in \mathbb{N} \text{ 対して，} n \in \bar{B} \text{となる} \tag{$*$}$$

ことを示す。今の場合， $P(n)$ は，”$n \in \bar{B}$” である。

(1) B は空ではないので，B の元 b が存在する。このとき，$1 \leqq b$ なので，$1 \in \bar{B}$ となる。

(2) $1, \ldots, n \in \bar{B}$ とする。ここで，$n+1 \notin \bar{B}$ 仮定する。すると，n は $\bar{B}$ の最大値になる。
実際，もし最大値でなければ，$n < m$ となる $\bar{B}$ の元 m が存在する。従って，$m \leqq x$ となる B の元 x が存在する。このとき，$n+1 \leqq m$ となるが，$n+1 \leqq m \leqq x$ なので，$n+1 \in \bar{B}$ となり仮定に反する。故に，n は $\bar{B}$ の最大値になるが，これは $\bar{B}$ の最大値がないという仮定に反する。従って，$n+1 \notin \bar{B}$ という仮定は誤りで，$n+1 \in \bar{B}$ となる。

(1), (2) より，数学的帰納法 2 を用いて，$\bar{B} = \mathbb{N}$ が得られる。しかし，これは $\bar{B}$ が有界であることに矛盾する。以上から，$\bar{B}$ には最大値が存在すること，従って，B に最大値が存在することが得られた。 □

2.2 除法の定理

自然数や整数での除法については次の定理が基本的で，この定理から多くの事実が示されます。

自然数での除法の定理

$n, m \in \mathbb{N}$ とする。このとき，

$$m = qn + r,\ \ 0 \leqq r < n$$

となる非負整数 q, r が唯 1 組存在する。この q を m を n で割ったときの商， r を余り（剰余）という。

自然数での除法の定理は整数に自然に拡張されます。

整数での除法の定理

$n, m \in \mathbb{Z}, n \neq 0$ とする。このとき，

$$m = qn + r,\ \ 0 \leqq r < |n|$$

となる整数 q, r が唯 1 組存在する。この，q を m を n で割った時の商，r を最少非負剰余，あるいは（$r \neq 0$ のとき,）最小正剰余と言う。

除法の定理は，自然数の基本的性質を使って証明することは可能ですが，厳密な証明には，自然数の基本的性質の正確な定式化が必要で，幾分煩雑です。この性質はよく知られているので，ここでは，証明は省略することにします。

いくつか例をあげましょう。

例 2.2.

(1) $30 = 4 \cdot 7 + 2$　　(2) $-30 = -5 \cdot 7 + 5$

(3) $30 = -4 \cdot (-7) + 2$　　(4) $-30 = 5 \cdot (-7) + 5$

2.3 整除性

除法の定理を使って自然数や整数の性質を調べるとき，重要な性質は「割り切れる」という性質，**整除性**です。

定義 2.1 (整除性)**.** $a, b \in \mathbb{Z}\ (a \neq 0)$ とする。$b = ca$ となる $c \in \mathbb{Z}$ が存在するとき，a は b を**割り切る**と言って，$a \mid b$ と表す。このとき，a は b の**約数**，b は a の**倍数**と言う。以後，$a \mid b$ と書いたときは，$a, b \in \mathbb{Z}\ (a \neq 0)$ を意味するものとする。

$b = 0$ の場合は，$0 = 0 \cdot a$ ですから，

すべての $a \neq 0$ に対して，$a \mid 0$

となります[*10]。また，整除性は符号に関係しない，即ち，

$$a \mid b \iff \pm a \mid \pm b$$

となることに注意しましょう。更に，整除性についての次の性質は基本的です。

命題 2.1. $a, b, c, x, y \in \mathbb{Z}$ に対して次が成立する。

(1) $a \mid b,\ a \mid c$ ならば，$a \mid (bx + cy)$

(2) $a \mid b,\ b \mid c$ ならば，$a \mid c$

(3) $a \mid b\ (b \neq 0)$ ならば，$|a| \leqq |b|$

(4) $a \mid b,\ b \mid a$ ならば，$|a| = |b|$

証明 (1) $a \mid b,\ a \mid c$ とすると，$k, l \in \mathbb{Z}$ に対して，$b = ka$，$c = la$ と表される。このとき，

$$bx + cy = kax + lay = (kx + ly)a$$

と表されるから，$a \mid (bx + cy)$ となる。

(2) $a \mid b,\ b \mid c$ とすると，$k, l \in \mathbb{Z}$ に対して，$b = ka$，$c = lb$ と表される。このとき，

$$c = lb = lka$$

と表されるから，$a \mid c$ となる。

(3) $a \mid b$ とすると，$k \in \mathbb{Z}$ に対して，$b = ka$ と表される。このとき，$|b| = |k| \cdot |a|$ で，$|k| \geqq 1$ より，

$$|a| \leqq |b|$$

が得らる。

(4) (3) を使うと，$a \mid b$ より，$|a| \leqq |b|$ が得られ，$b \mid a$ より，$|b| \leqq |a|$ が得られる。

□

上の命題 (1) で，x, y は負でも良いことに注意しましょう。

例 2.3. $a \mid 15$ かつ，$a \mid 6$ ならば，$a \mid 3$ となる。

実際，$15 - 2 \cdot 6 = 3$ より，上の命題 (1) より，$a \mid 3$ となる。

[*10] 約束により，$0 \mid 0$ は考えません。

2.4 最大公約数

2 つの自然数 a，b を測るときの最も大きな共通尺度（最大公約数）は，a，b を比較する際の基本的量で，古くから調べられてきました。実際，ユークリッドの「原論」には以下に説明する，最大公約数や素数の性質の多くが既に述べられています。

最大公約数

$a, b \in \mathbb{Z}$ とし，a, b のうち少なくとも一方は 0 でないとする。a と b の自然数の公約数[*11] で，最大のものを，a と b の**最大公約数**と言い，$\gcd(a, b)$ と表す。

例 2.4. 6 と 10 の最大公約数は 2 である。

実際，6 の自然数の約数は，$1, 2, 3, 6$ で，10 の自然数の約数は，$1, 2, 5, 10$ である。従って，6 と 10 の公約数は，$1, 2$ で，最大公約数は 2 となる。

最大公約数の存在は，その定義からほぼ明らかですが，証明の練習を兼ねて，証明をあげましょう。

命題 2.2. $a, b \in \mathbb{Z}$ とし，a, b のうち少なくとも一方は 0 でないとする。このとき，a と b の最大公約数 $\gcd(a, b)$ が存在する。

証明 $a \neq 0$，$b = 0$ のとき，$a \mid 0$ だから，この場合，$\gcd(a, 0) = |a|$ で確かに最大公約数は存在する。

そこで，$a, b \neq 0$ とする。a, b の自然数の公約数の成す集合を C とする。$x \in C$ とすると，x は，$x \mid a$ かつ，$x \mid b$ だから，$x \leqq \min(|a|, |b|)$ となる。即ち，C は空でない上に有界な自然数の集合である。従って，$\mathbb{N}$ の有界集合での最大値の存在性より，C の最大値，即ち，a と b の最大公約数が存在する。 □

最大公約数の存在は上の命題で分かりますが，この命題からは実際にどのように求めるかは分かりません。実は，最大公約数はユークリッドの互除法を使うと効率的に求めることができます。ユークリッドの互除法については別項に説明がありますので，そちらを参照してください。

[*11] a の約数かつ b の約数であるものを，a, b の**公約数**と言います。

2.5 素数

素数は数を乗法的に見たときの構成要素で，整除性を調べる際の基本的要素です。

定義 2.2. （素数）1 と 自分自身以外の約数を持たない自然数 (> 1) を**素数**という。そうでない自然数 (> 1) を**合成数**と言う。[*12]

素数の定義から，次が成立することが分かります。

p を素数とし, $a \in \mathbb{N}(a > 1)$ とする。このとき，$a \mid p$ ならば $a = p$ である。

例 2.5. $2, 3, 5, 7$ は素数，$4, 6, 9$ は合成数である。

素数についての次の性質は基本的です。

命題 2.3. p を素数とする。自然数 a, b に対して，

$$p \mid ab \quad \text{ならば，} \quad p \mid a \quad \text{または} \quad p \mid b$$

である。

この命題は普通，拡張ユークリッドの互除法の結果を用いて証明されます。拡張ユークリッドの互除法については，別項で説明がありますが，ここではそれを使わないで，除法の定理から，数学的帰納法を使って，直接証明しましょう。

ユークリッドの互除法は，深い結果ですから，それを使わない証明は多少複雑になります。

証明 すべての自然数 n に対して，

$$n \text{ 以下のすべての素数 } p \text{ が，命題の主張 "} p \mid ab \text{ ならば， } p \mid a \text{ または } p \mid b \text{ "を満たす} \qquad (*)$$

ことを，数学的帰納法で証明する。

(1) $n = 1$ のときは，n 以下の素数は存在しないから，$(*)$ は成立する。

(2) n のとき，$(*)$ が成立と仮定する。このとき，$n+1$ について $(*)$ が成立することを示す。$n+1$ が合成数のときは，$n+1$ 以下の素数と n 以下の素数は同じだから，$(*)$ は成立する。

そこで，$n + 1 = q$ を素数とする。

$$q \mid ab \text{ で } q \nmid a \text{ かつ } q \nmid b \qquad (**)$$

となる，自然数 a, b が存在したとする。そのような組 a, b の中で，ab が最小となる組 a, b を一組取り，それを改めて a, b とする。このとき，$a, b > 1$ である。a，b をそれぞれ q で割り余りを r_1, r_2 とする。即ち，

$$a = q_1 q + r_1, \quad 0 < r_1 < q$$
$$b = q_2 q + r_2, \quad 0 < r_2 < q$$

[*12] 負の数も含めて素数や合成数の用語を用いる立場もあります。

とする。仮定 $q \nmid a$, $q \nmid b$ から，$r_1, r_2 \neq 0$ となる。このとき，

$$r_1 r_2 = (a - q_1 q)(b - q_2 q) = ab + (q_1 q_2 q - a q_2 - b q_1) q$$

で $q \mid ab$ なので，$q | r_1 r_2$ が得られる。ここで，$q_1 \neq 0$ または，$q_2 \neq 0$ なら，$r_1 r_2 < ab$ となり，ab の取り方の最小性に反するので，$q_1 = q_2 = 0$ で，$r_1 = a$, $r_2 = b$ となる。

そこで，$qc = r_1 r_2$ $(c > 1)$ と表すことができる。c の一つの素因数を，p とすると，$c = ps$ で，

$$p \mid r_1 r_2$$

となる。ここで，$0 < r_1, r_2 < q$ かつ $r_1 r_2 = ab = qc$ なので，$c < q$ で，従って，$p < q = n + 1$ となる。故に帰納法の仮定から，$p \mid r_1$ または $p \mid r_2$ が得られる。

$p \mid r_1$ の場合，$pd = r_1$ と書けるので，このとき，$qps = qc = r_1 r_2 = p d r_2$ の両辺を p で割って，$qs = d r_2$ となる。ここで，$0 < d < r_1 < q$ なので，$q \nmid d$ となり，以上から

$$q \mid d r_2 \text{ で } q \nmid d \text{ かつ } q \nmid r_2$$

となる組 d, r_2 が得られた。ここで，$d r_2 < r_1 r_2 = ab$ なので，ab の最小性に反し矛盾である。

$p \mid r_2$ の場合もまったく同様にして矛盾が得られる。

以上から，(∗∗) を満たす a, b は存在しない。即ち，$n + 1$ の場合も (∗) が成立することが得られた。

以上から，すべての n に対して，(∗) が成立することが得られた。 □

この命題から，素因数分解の一意性の証明に用いられる次の系が得られます。

系 2.1. $p, p_1, \ldots, p_r$ を素数とし，

$$p \mid p_1 \cdots p_r$$

ならば，ある i $(1 \leqq i \leqq r)$ に対して，$p = p_i$ となる。

証明 r についての数学的帰納法を使って証明する。

(1) $r = 1$ のときは，$p \mid p_1$ より，$p = p_1$ となる。

(2) $r = n$ のとき主張が成立と仮定する。このとき，

$$p \mid p_1 \cdots p_{n+1} = p_1 \cdot (p_2 \cdots p_{n+1})$$

とみると，命題から，$p \mid p_1$ または，$p \mid p_2 \cdots p_{n+1}$ となる。$p \mid p_1$ の場合は，$p = p_1$ となり，$p \mid p_2 \cdots p_{n+1}$ の場合は，帰納法の仮定[*13]から，ある i $(2 \leqq i \leqq n + 1)$ に対して，$p = p_i$ となる。

以上，(1), (2) より，すべての自然数 r に対して，系が成立することが分かった。 □

[*13] n 個の素数 $p_2 \cdots p_{n+1}$ の積についての仮定。

2.6 素因数分解の一意性

素因数分解の一意性は，初等整数論での基本定理とも考えられる重要な性質です。素因数分解は中学校でも説明されている，よく知られている事柄ですが，高等学校でもその事柄の厳密な証明はされていないようです。

ここでは，前節の命題 2.3 を使って，証明しましょう。この証明は，標準的な初等整数論の教科書で普通に行われている最も標準的な証明です。

素因数分解の一意性

$n \in \mathbb{N},\ n > 1$ とする。このとき，n は相異なる有限個の素数 $p_1 < p_2 < \cdots < p_r$ に対して，

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r} \qquad (e_i \in \mathbb{N},\ e_i > 0) \tag{$*$}$$

と唯一通りに表される。

証明 [**存在性の証明**] 必ずしも異ならない s 個の素数 $p_1, \ldots p_s$ に対して，

$$n = p_1 \cdot p_2 \cdots p_s \tag{$*2$}$$

と表されることを示せば十分である。

(1) $n = 1$ は条件を満さないので，(∗2) は成立する[*14] 。

(2) $1, \ldots, n$ まで (∗2) が成立したと仮定する[*15]。このとき，$n+1$ が (∗2) を満たすことを示す。

まず，$n+1$ が素数なら，$n+1 = n+1$ が素因数分解になっているから，(∗2) は成立する。

次に，$n+1$ を合成数とする。このとき，自然数 $x, y > 1$，に対して $n+1 = xy$ と書ける。ここで，$x, y < n+1$ だから，$x, y \leqq n$ となり，帰納法の仮定から，x, y は (∗) を満たす。従って，

$$x = p_1 \cdots p_t,\quad y = p_{t+1} \cdots p_u$$

と表される。故に，

$$n+1 = xy = p_1 \cdots p_t, \cdot p_{t+1} \cdots p_u$$

と書け，この場合も，$n+1$ が (∗2) を満たすことが示された。

以上，(1), (2) より，存在性が証明された。

[**一意性の証明**] $n > 1$ が (∗) の形に一意的に表されることを，やはり数学的帰納法 2 を使って証明する。

(1) $n = 1$ は条件を満たさなので，主張は成立する。

[*14] この論法に違和感を感じる人がいるかも知れません。実はこの場合，数学的帰納法を適用している命題は，

$$n > 1 \text{ のとき，}\quad n = p_1 \cdot p_2 \cdots p_s \tag{$*2'$}$$

です。「$n > 1$ のとき,」は $n = 1$ のときは特に条件を課さない主張を意味します。つまりこの場合は無条件に (∗2′) は成立と考えてよいとなります。このような数学的帰納法を使う場合は，$n = 2$ からスタートするとして，$n = 2$ の場合を示すという方法もあります。しかし，(2) の証明を見ると，実は $n = 2$ の場合も含まれるものになっていますので，ここでは数学的帰納法 2 に忠実な形に述べました。

[*15] 以下の証明は $n = 1$ の場合，即ち 2 が (∗2) を満たすこと，も含んでいることに注意しましょう。

(2) $1,\ldots,n$ について，$(*)$ の形に一意的に表されると仮定する。

$n+1$ の素因数分解を素数 $p_1 < p_2 < \cdots < p_r$，$q_1 < q_2 < \cdots < q_r$ に対して，

$$n+1 = p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r} = q_1^{f_1} \cdot q_2^{f_2} \cdots q_s^{f_s} \quad (e_i, f_j \in \mathbb{N},\ e_i, f_j > 0) \tag{*3}$$

とする。ここで，$p_1 \leqq q_1$ と仮定する[*16]。このとき，

$$p_1 \mid q_1^{f_1} \cdot q_2^{f_2} \cdots q_s^{f_s}$$

だから，系 2.1 より，ある i に対して，$p_1 = q_i$ となるが，$p_1 \leqq q_1 < q_2 < \ldots$ より，$p_1 = q_1$ となる。そこで，$p_1 = q_1$ で $(*3)$ の両辺を割ると

$$\frac{n+1}{p_1} = p_1^{e_1-1} \cdot p_2^{e_2} \cdots p_r^{e_r} = q_1^{f_1-1} \cdot q_2^{f_2} \cdots q_s^{f_s} \tag{*4}$$

が得られる。ここで $\frac{n+1}{p_1} < n+1$ より，帰納法の仮定から $(*4)$ の素因数分解は一意で，

$$r = s,\ p_i = q_i,\ e_i = f_i\ (1 \leqq i \leqq s)$$

となる。従って，$(*3)$ の 2 項，3 項の分解は同じになる。

以上より，$(*)$ の分解の一意性が示された。 □

素因数分解の一意性は数論の中で色々な場面で使われますが，ここでは応用例として，素数の基本的性質を２つ示しましょう。

まず，素数性の判定でよく使われる次の性質です。

命題 2.4. 自然数 $n > 1$ が合成数ならば，n の素因数 p で $p^2 \leqq n$ となるものが存在する。

証明 n は合成数なので，$n = ml$，$(1 < m \leqq l < n)$ と表される。そこで，m の素因数を p とすると，$p^2 = p \cdot p \leqq m \cdot l = n$ となる。 □

この命題の対偶を取ると，次が得られます。

素数判定

自然数 n が，$\sqrt{n}$ 以下のすべての素数で割り切れなければ，n は素数である。

簡単な例を挙げましょう。

例 2.6. 101 は素数である。

実際，$\sqrt{101} < 11$ より，$\sqrt{101}$ 以下の素数は，$2, 3, 5, 7$ である。101 はこれらのいずれでも割り切れないから，素数である[*17]。

素因数分解の性質から得られる別の結果として，素数の無限性があります。

[*16] もし，$p_1 > q_1$ なら，p_i と q_j を入れ替えて考えます。

[*17] 全く同様にして，$103, 107, 109, 113$ も素数であることが分かります。

定理 2.1 (ユークリッド)**.** 素数は無限に存在する[*18]。

証明 素数が有限 M 個しかないと仮定する。このとき，すべての素数を $p_1, p_2, \ldots, p_M$ と表し，$L = p_1 \cdot p_2 \cdots p_M + 1$ と置く。L の素因数の一つを q とすると，q は $p_1, p_2, \ldots, p_M$ のいずれとも異なる。実際，もしある i に対して，$p_i = q$ ならば，$L - p_1 \cdot p_2 \cdots p_M = 1$ の左辺は $p_1 = q$ で割り切れ，それは 1 を割り切ることになり，矛盾である。 □

この証明によれば，L の素因数は $p_1, p_2, \ldots, p_M$ と異なることが分かります。例えば次が得られます。

例 2.7. $L = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031$ の素因数は $2, 3, 5, 7, 11, 13$ と異なる。
実際，$30031 = 59 \cdot 509$ と素因数分解され，素因数は $59, 509$ である。

「記号と準備」更新記録

- (2017 年 06 月版)　数学的帰納法 1,2 の同値性の証明の追加，基本的素数判定の方法，素数の無限性の証明の追加。証明での文体を「である調」に変更。
- (2014 年 06 月版) 初版公開

[*18] この結果はユークリッド「原論」第 9 巻命題 20 にあることから，ユークリッドの定理とも呼ばれます。