

## 0 「数学 (2010 年度)」の講義について

この講義で取り扱う内容は

- ・ 集合
- ・ 命題と論理
- ・ 写像と集合の濃度
- ・ 代数学の話 (整数の話)

以下は時間があれば、取り扱う .

- ・ 幾何学の話 (一筆書きや多面体の Euler の定理など)
- ・ 解析学の話 (数列と関数の極限 , 実数の話)

を扱う予定 .

教材はプリントを授業の時に配布するとともに , インターネットにて配布する . PDF ファイルなので , Acrobat Reader が必要 (たいていのパソコンにはインストールされている)

ホームページのアドレスは

<http://kitty-shiro.sakura.ne.jp/>

または

<http://kitty-shiro2.sakura.ne.jp/>

mail address : [ibuki@econ.u-hyogo.ac.jp](mailto:ibuki@econ.u-hyogo.ac.jp)

[k.ibuki@ezweb.ne.jp](mailto:k.ibuki@ezweb.ne.jp)(ケイタイからのメールのみ受信可能)

### 関連図書

- [1] 樋口禎一ほか著「現代数学の基礎」牧野書店 1994 年  
数理情報科学シリーズ 7 1,700 円
- [2] Neal Koblitz, *A Course in Number Theory and Cryptography*  
(second edition), Springer, 1994 年
- [3] 小川 洋子, 「博士の愛した数式」, 新潮社, 2003 年 1,500 円 (文庫本あり?)
- [4] サイモン・シン, 「フェルマーの最終定理—ピュタゴラスに始まり、ワイルズが証明するまで」 青木薫訳、新潮社、2000 年 2,450 円 (文庫本あり 820 円)

[1] は 5 年前のこの講義のテキスト . この授業で配布するプリントはこの本の内容と重複することが多い . [2] は整数と暗号を扱った本で , 英語で書かれた数学的には高度な本 . このプリントの代数学の話 (整数の話) の部分はこの本の一部の翻訳 . [3] は整数の話を盛り込んだ小説 (映画化されたベストセラー) . [4] はフェルマー予想が解決するまでのさまざまな話題について触れているノンフィクション .

# 1 集合

## 1.1 集合の記号

ものの集まりで、それに属しているか属していないかが定まっているものを 集合 (set) という。集合を表わす記号は中括弧 ( $\{ \}$ ) を用いて、

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

のように列挙したり、

$$\{n \mid n \text{ は } 0 \text{ 以上で } 10 \text{ 未満の整数}\}$$

$$\{n^2 \mid n \text{ は自然数}\}$$

のように、

$$\{\text{変数の式} \mid \text{変数に関する条件}\}$$

の形で表わす。

集合そのものは  $A$  や  $B$  のようにアルファベットの大文字で表わすことが多い。

$$A = \{n \mid n \text{ は } 0 \text{ 以上で } 10 \text{ 未満の整数}\}, \quad B = \{n^2 \mid n \text{ は自然数}\}$$

集合を構成しているものを 要素 とか 元 という。

### よく用いられる数の集合の記号

$N$  : 自然数 (natural number) の全体

$Z$  : 整数 (integer) の全体 (ドイツ語の Zahlen(数) からきている)

$Q$  : 有理数 (rational number) の全体 (Quotient(商) からきている)

$R$  : 実数 (real number) の全体

$C$  : 複素数 (complex number) の全体

$a$  が  $A$  の元であるとき、すなわち、 $a$  が  $A$  に属しているとき、

$$a \in A \quad \text{あるいは} \quad A \ni a$$

と書く。また、 $a$  が  $A$  に属していないときは、

$$a \notin A \quad \text{あるいは} \quad A \not\ni a$$

と書く。

2つの集合  $A$  と  $B$  に対して  $A$  の元がすべて  $B$  の元でもあるとき、すなわち、 $A$  に属している元がすべて  $B$  にも属しているとき、

$$A \subset B \quad \text{あるいは} \quad B \supset A$$

と書き、 $A$  は  $B$  に含まれる とか  $A$  は  $B$  の部分集合 (subset) である という。

$A$  が  $B$  に含まれないとき、すなわち、 $A$  に属してはいるが、 $B$  には属さない元があるとき、

$$A \not\subset B \quad \text{あるいは} \quad B \not\supset A$$

と書く .

$A \subset B$  かつ  $A \supset B$  であるとき ,  $A$  と  $B$  は等しい といい ,  
 $A = B$

と書く .

$A \subset B$  ではあるが ,  $A$  と  $B$  が等しくない ( $A \neq B$ ) とき ,  $A$  は  $B$  の真部分集合である  
 といい ,

$$A \subsetneq B \quad \text{あるいは} \quad B \supsetneq A$$

と表わす .

次の 2 つの定理が成り立つことは容易に分かる .

定理 1.1

- (1)  $A = A$
- (2)  $A = B$  ならば  $B = A$
- (3)  $A = B$  かつ  $B = C$  ならば  $A = C$

定理 1.2

- (1)  $A \subset A$
- (2)  $A \subset B$  かつ  $B \subset C$  ならば  $A \subset C$

## 1.2 集合の演算

和集合

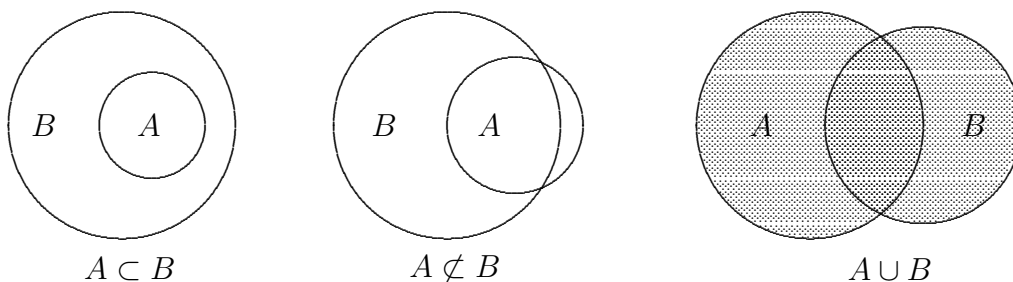
集合  $A$  の元と集合  $B$  の元を併せた集合を  $A$  と  $B$  の 和集合 (union) といい ,

$$A \cup B$$

と表わす , すると  $A \cup B$  は , 次のようなものである .

$$A \cup B = \{x \mid x \in A \quad \text{または} \quad x \in B\}$$

次のように , 集合を図で表現したものを Venn 図 という .



次の定理が成り立つ .

定理 1.3

- (1)  $A \subset A \cup B$  ,  $B \subset A \cup B$
- (2)  $A \cup B = B \cup A$
- (3)  $(A \cup B) \cup C = A \cup (B \cup C)$
- (4)  $A \subset B \Leftrightarrow A \cup B = B$

問 1 定理 1.3 の (4) を証明しなさい .

共通部分

集合  $A$  と集合  $B$  の両方に属する元からなる集合を  $A$  と  $B$  の 共通部分 (intersection) といい ,

$$A \cap B$$

と表わす , すると  $A \cap B$  は , 次のようなものである .

$$A \cap B = \{x \mid x \in A \text{ かつ } x \in B\}$$

次の定理が成り立つ .

定理 1.4

- (1)  $A \cap B \subset A$  ,  $A \cap B \subset B$
- (2)  $A \cap B = B \cap A$
- (3)  $(A \cap B) \cap C = A \cap (B \cap C)$
- (4)  $A \subset B \Leftrightarrow A \cap B = A$

問 2 定理 1.4 の (4) を証明しなさい .

また ,  $\cup$  と  $\cap$  の間には次の分配法則が成り立つ .

定理 1.5(分配法則)

- (1)  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- (2)  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

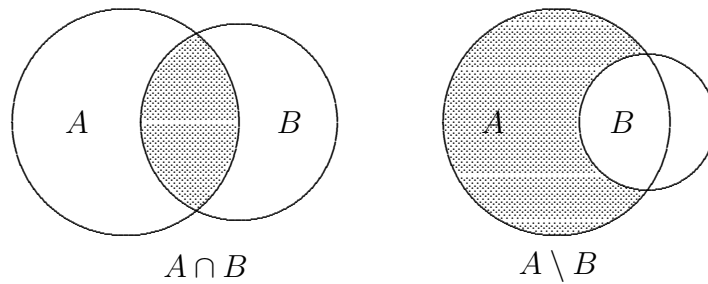
差集合

2つの集合  $A$  と  $B$  があるとき ,  $A$  に属して ,  $B$  に属さないものの全体を 差集合 といい ,

$$A \setminus B$$

と表わす . すなわち ,

$$A \setminus B = \{x \mid x \in A \text{ かつ } x \notin B\}$$

空集合，全体集合，補集合

属する元が1つも無いものも集合とみなしてこれを 空集合 (empty set) といい，

$$\emptyset$$

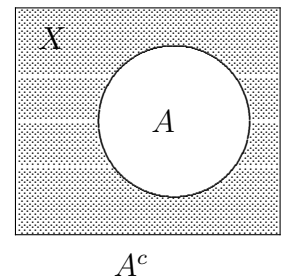
と表わす．

また，ある定まった集合  $X$  の中でその部分集合だけを考えるととき，この  $X$  を 全体集合 という．

全体集合  $X$  が定まっているとき，その部分集合  $A$  に対して  $X \setminus A$  を  $A$  の 補集合 (complement) といい，

$$A^c$$

と表わす (TEXT によっては  $\bar{A}$  と表わすことがある) ．



さらに，次の de Morgan の法則 が成り立つ．

**定理 1.6**(de Morgan の法則)

$$(1) \quad (A \cup B)^c = A^c \cap B^c$$

$$(2) \quad (A \cap B)^c = A^c \cup B^c$$

**問 3** 定理 1.6 を Venn 図を用いて確かめよ．

## 練習問題 1-1

全体集合を

$$X = \{\text{cat, rat, pig, dog, elephant, mouse, horse, cow, panda, zebra, bear, tiger}\}$$

また,  $A, B, C$  を  $X$  の部分集合で次のようなものとする.

$A$ :最後が母音 (a, e, i, o, u) で終わる英単語

$B$ :最初が c で始まる英単語

$C$ :文字 e を含む英単語

次の集合を求めよ.

- |                     |                     |                     |                     |
|---------------------|---------------------|---------------------|---------------------|
| (1) $A \cap B$      | (2) $A \cap C$      | (3) $B \cap C$      | (4) $A \cup B$      |
| (5) $A \cup C$      | (6) $B \cup C$      | (7) $C \setminus A$ | (8) $A^c$           |
| (9) $C^c$           | (10) $A^c \cup C^c$ | (11) $(A \cap C)^c$ | (12) $A^c \cap C^c$ |
| (13) $(A \cup C)^c$ |                     |                     |                     |

## 練習問題 1-2

全体集合を  $X = \{x \mid x \in \mathbb{Z} \text{ かつ } 0 \leq x \leq 100\}$  とする. また,

$$A = \{x \mid x \in X \text{ かつ } x \text{ は } 2 \text{ の倍数}\}$$

$$B = \{x \mid x \in X \text{ かつ } x \text{ は } 3 \text{ の倍数}\}$$

$$C = \{x \mid x \in X \text{ かつ } x \text{ は } 5 \text{ の倍数}\}$$

とすると, 次の集合の個数を求めよ. また, 個数が 10 個以下のものは元 (要素) をすべて列挙せよ.

- |                |                  |                  |                    |                     |
|----------------|------------------|------------------|--------------------|---------------------|
| (1) $A \cap B$ | (2) $A \cap C$   | (3) $B \cap C$   | (4) $A \cup B$     | (5) $A \cup C$      |
| (6) $B \cup C$ | (7) $A^c \cap C$ | (8) $A^c \cup C$ | (9) $B^c \cap C^c$ | (10) $(A \cap C)^c$ |

## 2 写像と集合の濃度

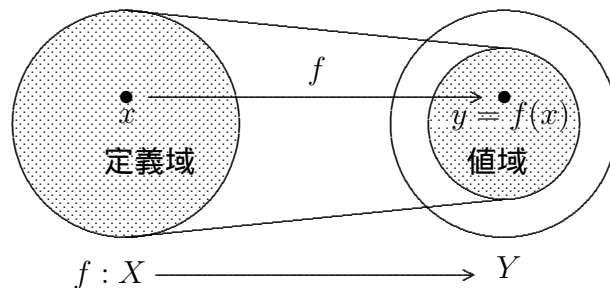
### 2.1 全射と単射

2つの集合  $X$  と  $Y$  について,  $X$  の勝手な元  $x$  に対して  $Y$  の元  $y$  が唯一つ定まるとき, この対応を  $X$  から  $Y$  への 写像 (mapping または map) という. この写像を  $f$  で表わすとき,  $x$  に対応する  $Y$  の元  $y$  を  $f(x)$  と表わし,  $x$  の写像  $f$  による 像 (image) という. また,  $X$  を 定義域,  $X$  の  $f$  による像全体

$$\{f(x) \mid x \in X\}$$

を 値域 といい,  $f(X)$  と表わすことにする.

集合  $X$  と  $Y$  が数の集合のとき, 写像を 関数 (function) という ( $X$  が数の集合でないときも関数ということがある).



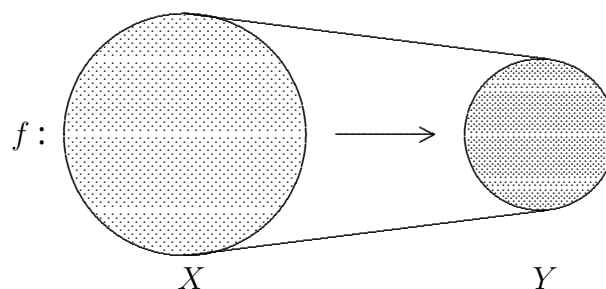
#### 恒等写像 (identity mapping)

集合  $X$  から  $X$  への写像で  $X$  の任意の元  $x$  に対して, 自分自身  $x$  を対応させる写像を 恒等写像 といい,  $id_X$  と表わす.

$$id_X : X \rightarrow X, \quad id_X(x) = x \text{ for } x \in X$$

#### 全射

集合  $Y$  の勝手な元  $y$  に対して,  $y = f(x)$  となるような  $X$  の元  $x$  があるとき, 写像  $f$  は 全射 であるという. このことは,  $X$  が写像  $f$  によって  $Y$  全体に写されていることを意味する. すなわち,  $f(X) = Y$  となっている.



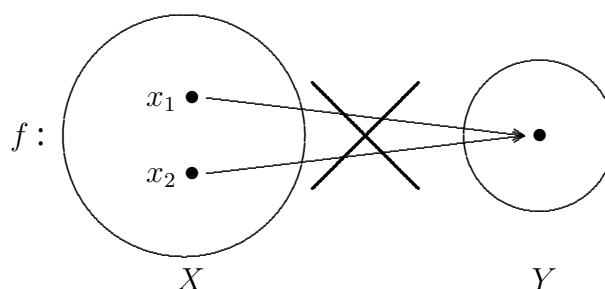
単射

集合  $X$  の勝手な 2 つの元  $x_1$  と  $x_2$  に対して,

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

となっているとき, 写像  $f$  は単射であるという. 言い換えると(対偶をとると),

$$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$$



また, 集合  $X$  から集合  $Y$  への写像  $f$  が全射でありかつ単射になっているとき,  $f$  は全単射(または1対1の対応)であるという.

**練習問題 2-1** 次の写像  $f: X \rightarrow Y$  は全射になっているか, 単射になっているかを調べよ. 全射になっていない場合や単射になっていない場合にはその理由を説明しなさい.

(1)  $f: X = [0, \infty) = \{x \mid 0 \leq x\} \rightarrow Y = \mathbf{R} \quad y = f(x) = x^2 + 1$

(2)  $f: X = \{0, 1, 2, 3, 4, 5\} \rightarrow Y = \{0, 1, 2, 3, 4, 5\}$

$y = f(x) = x$  を 2 倍して 6 で割った余り

**練習問題 2-2** 次の写像は全射になっているか, 単射になっているかを調べよ.

(1)  $f: X = \mathbf{N} \rightarrow Y = 2\mathbf{N} \quad y = f(x) = 2x + 10$

(2)  $f: X = \mathbf{N} \rightarrow Y = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$y = f(x) = x$  を 10 で割った余り

(3)  $f: X = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} \rightarrow Y = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$y = f(x) = x$  を 3 倍して 10 で割った余り

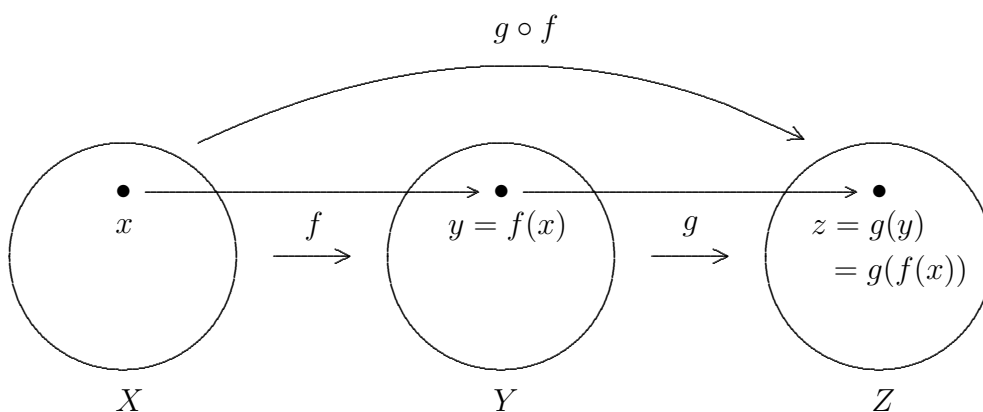
(4)  $f: X = \{\text{cat}, \text{dog}, \text{panda}, \text{zebra}, \text{puma}, \text{tiger}\} \rightarrow Y = \{\text{a}, \text{e}, \text{i}, \text{o}, \text{u}\}$

$y = f(x) = x$  の最初の母音

上で, 全射になっていないものは,  $Y$  から適当に要素を取り除き, 全射になるようにしなさい. また, 単射になっていないものは,  $X$  から適当に要素を取り除き, 単射になるようにしなさい.

合成写像

集合  $X$  から集合  $Y$  への写像  $f$  と  $Y$  から集合  $Z$  への写像  $g$  が与えられているとき,  $X$  の元  $x$  を  $f$  によって  $Y$  の元  $f(x)$  に写し, さらにこれを  $g$  によって  $Z$  の元  $g(f(x))$  に移すことによって,  $X$  から  $Z$  への写像が出来る. この写像を  $f$  と  $g$  の 合成写像 といい,  $g \circ f$  で表わす.

逆写像

集合  $X$  から集合  $Y$  への写像  $f$  が全単射になっているとき,  $Y$  の任意の元  $y$  に対して,  $y = f(x)$  となるような  $X$  の元  $x$  が唯一つ定まる. このような  $y$  から  $x$  が定まる対応を  $f$  の 逆写像 といい,  $f^{-1}$  で表わす.

$$f^{-1}(f(x)) = x \text{ for } x \in X, \text{ すなわち } f^{-1} \circ f = id_X$$

$$f(f^{-1}(y)) = y \text{ for } y \in Y, \text{ すなわち } f \circ f^{-1} = id_Y$$

次の定理が成り立つ.

**定理 2.1**  $f: X \rightarrow Y, g: Y \rightarrow Z$  とする.

- (1)  $g \circ f: \text{全射} \Rightarrow g: \text{全射}$
- (2)  $g \circ f: \text{単射} \Rightarrow f: \text{単射}$
- (3)  $Z = X$  とし,  $g \circ f: \text{全単射}$  かつ  $f \circ g: \text{全単射} \Rightarrow f$  と  $g$  は全単射

**練習問題 2-3** 次の2つの写像  $f: X \rightarrow Y, g: Y \rightarrow Z$  の合成写像  $g \circ f$  を作りなさい.

$$(1) X = \mathbf{R}, Y = \mathbf{R}, Z = \mathbf{R}, y = f(x) = a^x, z = g(y) = \frac{1}{y^2 + 1}$$

$$(2) X = \{\text{cat}, \text{dog}, \text{panda}, \text{zebra}, \text{puma}\}$$

$Y: \text{アルファベット 26 文字}$

$$Z = \mathbf{N}$$

$y = f(x) = x$  の3番目の文字,  $z = g(y) = y$  の abc 順による順番

$g \circ f(\text{cat}), g \circ f(\text{dog}), g \circ f(\text{panda}), g \circ f(\text{zebra}), g \circ f(\text{puma})$  を求めよ.

練習問題 2-4 次の写像  $f: X \rightarrow Y$  は全単射になっている.  $y = f(x)$  の逆写像  $x = f^{-1}(y)$  を作りなさい.

$$(1) \quad X = [0, 1) \quad , \quad Y = [1, \infty) \quad y = f(x) = \frac{1}{1-x}$$

$$(2) \quad X = \mathbf{R} \quad , \quad Y = \mathbf{R} \quad y = f(x) = \frac{10^x - 10^{-x}}{2}$$

## 2.2 集合の濃度 (個数の拡張)

集合  $X$  が有限集合のときその個数  $n$  を 濃度 と呼び,  $\#X$  で表わすことにする. このことは, 集合  $X$  から次の集合

$$\{1, 2, 3, \dots, n\}$$

への全単射が存在することを意味する.

例 1  $A = \{a, b, c, \dots, z\}$  ,  $Y = \{1, 2, 3, \dots, 26\}$  とすれば,  $A$  から  $Y$  への次のような全単射  $f$  がある.

$$f(a) = 1, f(b) = 2, f(c) = 3, \dots, f(y) = 25, f(z) = 26$$

このような全単射は一通りではない. ほかに, 次のような  $g$  や  $h$  を考えてもよい.

$$g(z) = 1, g(y) = 2, g(x) = 3, \dots, g(b) = 25, g(a) = 26$$

$$h(b) = 1, h(c) = 2, h(d) = 3, \dots, h(z) = 25, h(a) = 26$$

これらのことから,  $\#A = 26$  である.

無限集合の場合も, 2つの集合  $X$  と  $Y$  に対して,  $X$  から  $Y$  への全単射が存在するとき, 2つの集合の濃度  $\#X$  と  $\#Y$  は等しいと定め,  $\#X = \#Y$  と書く.

自然数全体の集合  $N$  を 可算濃度 といい,  $\aleph_0$  (アレフゼロ) と書く.

例 2 (1) 正の偶数全体の集合  $2N$  の濃度は可算濃度  $\aleph_0$  である.

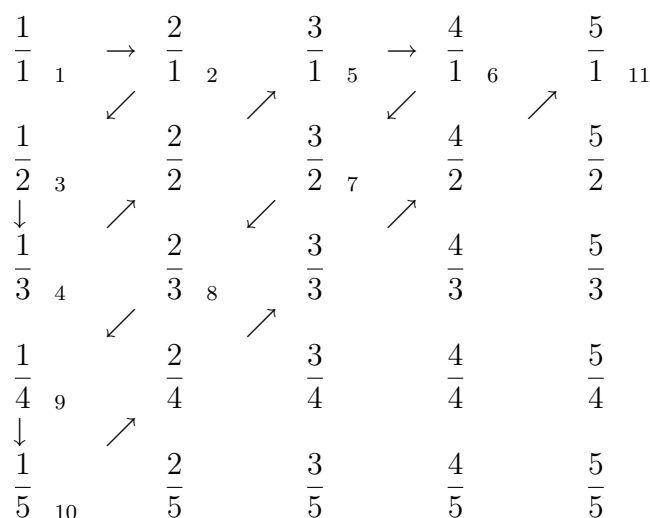
$$f: N \rightarrow 2N (\text{全単射}), \quad y = f(n) = 2n$$

(2) 整数全体の集合  $Z$  の濃度は可算濃度  $\aleph_0$  である.

$$\begin{array}{cccccccc} N & \cdots & \textcircled{5} & \textcircled{3} & \textcircled{1} & \textcircled{2} & \textcircled{4} & \cdots \\ Z & \cdots & -2 & -1 & 0 & 1 & 2 & \cdots \end{array}$$

$$f: N \rightarrow Z (\text{全単射}), \quad y = f(x) = \begin{cases} n/2 & n: \text{正の偶数のとき} \\ -(n-1)/2 & n: \text{正の奇数のとき} \end{cases}$$

(3) 正の有理数全体の集合の濃度は可算濃度  $\aleph_0$  である .



(4) 有理数全体  $Q$  の集合の濃度は可算濃度  $\aleph_0$  である .

問1 例1の(4)を証明しなさい .

定義 2つの集合  $X$  と  $Y$  に対して,  $X$  から  $Y$  への単射が存在するとき,

$$\#X \leq \#Y$$

と定める . また,  $\#X \leq \#Y$  であって,  $\#X \neq \#Y$  であるとき,  $\#X < \#Y$  と書こう .

定理 2.2 2つの集合  $X$  と  $Y$  に対して,  $X$  から  $Y$  への全射が存在すれば,  $Y$  から  $X$  への単射が存在し,  $\#Y \leq \#X$  が成り立つ .

定理 2.3(Cantor-Bernstein) 2つの集合  $X$  と  $Y$  に対して,  $X$  から  $Y$  への単射と全射が存在すれば,  $X$  から  $Y$  への全単射が存在し,  $\#X = \#Y$  が成り立つ . このことから,  $X$  から  $Y$  への単射と全射が存在すれば, 2つの集合の濃度は等しいことがわかる .

このことは,  $\#X \leq \#Y$  かつ  $\#X \geq \#Y$  が成り立てば,  $\#X = \#Y$  が成り立つことも示している .

定理 2.4 任意の2つの集合  $X$  と  $Y$  に対して,  $\#X \leq \#Y$  または  $\#X \geq \#Y$  が成り立つ .

定理 2.2, 定理 2.3 . 定理 2.4 の証明は難しいので省略する .

実数の濃度 (連続体の濃度)

集合  $I$  を 0 と 1 の間の実数全体とする．すなわち，

$$I = \{x \mid x \in \mathbf{R} \text{ かつ } 0 < x < 1\}$$

$n \in \mathbf{N}$  に対して， $f(n) = 1/n$  とすると，これは  $\mathbf{N}$  から  $I$  への単射となっている．このことと，定理 1.8 より， $\aleph_0 \leq \#I$  である．しかし， $\#I \neq \aleph_0$  であることを以下に示そう．

背理法によって示す． $\#I = \aleph_0$  とすると， $\mathbf{N}$  から  $I$  への全単射  $f$  が存在する． $f(n)$  を少数表示して，

$$\begin{aligned} f(1) &= a_1 = 0 . \underline{a_{11}} \ a_{12} \ a_{13} \ a_{14} \ a_{15} \ \cdots \\ f(2) &= a_2 = 0 . a_{21} \ \underline{a_{22}} \ a_{23} \ a_{24} \ a_{25} \ \cdots \\ f(3) &= a_3 = 0 . a_{31} \ a_{32} \ \underline{a_{33}} \ a_{34} \ a_{35} \ \cdots \\ f(4) &= a_4 = 0 . a_{41} \ a_{42} \ a_{43} \ \underline{a_{44}} \ a_{45} \ \cdots \\ f(5) &= a_5 = 0 . a_{51} \ a_{52} \ a_{53} \ a_{54} \ \underline{a_{55}} \ \cdots \\ &\dots\dots\dots \end{aligned}$$

ただし， $0.2 = 0.1999999 \cdots$  のように，無限小数でないものは 2 通りの表わし方があるが，無限小数として表わすことにする．

いま，アンダーライン部分の  $a_{ii}$  によって，次のように  $b_i$  を定める．

$$b_i = \begin{cases} 1 & a_{ii}: \text{偶数のとき} \\ 2 & a_{ii}: \text{奇数のとき} \end{cases}$$

$b = 0 . b_1 \ b_2 \ b_3 \ b_4 \ b_5 \ \cdots$  とおくと， $b$  はどの  $f(n)$  と異なるので， $f$  は全射になっていない(矛盾)．

このようにして， $I$  の濃度は  $\aleph_0$  より大きいことがわかる． $I$  から実数全体の集合  $\mathbf{R}$  へは全単射が存在するので， $\aleph_0 < \#I = \#\mathbf{R}$  となる．実数  $\mathbf{R}$  の濃度を 連続体の濃度 といい， $\aleph$  とか  $\aleph_1$  で表わす．

ベキ集合とベキ集合の濃度

集合  $X$  に対して空集合を含めた  $X$  の部分集合の全体を  $X$  のベキ集合といい  $2^X$  で表わす．

例 3  $X = \{1, 2, 3\}$  とする．すると，その部分集合全体  $2^X$  は

$$\begin{array}{ll} \emptyset & \longleftrightarrow 000 \\ \{1\} & \longleftrightarrow 100 \\ \{2\} & \longleftrightarrow 010 \\ \{3\} & \longleftrightarrow 001 \\ \{1, 2\} & \longleftrightarrow 110 \\ \{1, 3\} & \longleftrightarrow 101 \\ \{2, 3\} & \longleftrightarrow 011 \\ \{1, 2, 3\} & \longleftrightarrow 111 \end{array}$$

であり， $\#(2^X) = 2^3$

一般に， $X$  が有限集合で， $\#X = n$  とするとき， $\#(2^X) = 2^n$  である．また，連続体の濃度  $\#\mathbf{R}$  は  $\#(2^{\mathbf{N}})$  と等しい．

定理 2.5 集合  $X$  に対して,

$$\#X < \#(2^X)$$

である.

(証明)  $X$  から部分集合の集合  $2^X$  への写像

$$f: X \rightarrow 2^X, \quad f(x) = \{x\}$$

は単射となっているので,  $\#X \leq \#(2^X)$  が言える.

背理法で  $\#X \neq \#(2^X)$  を示そう. もし,  $\#X = \#(2^X)$  とすれば,  $X$  から  $2^X$  への全単射  $g$  が存在する. いま, 次のような  $X$  の部分集合  $A$  を考える.

$$A = \{x \mid x \notin g(x)\}$$

$g$  は全射であるので,  $X$  の元  $a$  で,  $g(a) = A$  となるものが存在する. この  $a$  が  $A$  に属しているのか属していないのかを調べよう.

もし,  $a \in A$  であるとすれば,  $a \in A = g(a)$  となり,  $a \notin A$  で矛盾.

もし,  $a \notin A$  であるとすれば,  $a \notin A = g(a)$  となり,  $a \in A$  で矛盾.

以上より,  $\#X \neq \#(2^X)$  が言え,  $\#X < \#(2^X)$  となることがわかる. (証明終)

「可算濃度  $\#N = \aleph_0$  と連続体濃度  $\#(2^N) = \aleph$  の間には別の濃度がない」という仮説がカントール (G. Cantor) によって 19 世紀に立てられた. これは「連続体仮説」と呼ばれているが, 20 世紀の半ば頃, クルト・ゲーデル (Kurt Godel) とポール・コーエン (Paul Cohen) によって, この仮説が成り立つとしても矛盾を生じない (成り立たないことを証明できない 1940 年ゲーデル) し, 成り立たないとしても矛盾を生じない (成り立つことを証明できない 1963 年コーエン) ことが示された.

練習問題 2-5 次の 2 つの集合  $X, Y$  は濃度が等しい.  $X$  から  $Y$  への全単射を作りなさい.

$$(1) X = (0, 1) = \{x \mid 0 < x < 1\}, \quad Y = (-1, 1) = \{y \mid -1 < y < 1\}$$

$$(2) X = (0, 1] = \{x \mid 0 < x \leq 1\}, \quad Y = [0, 2) = \{y \mid 0 \leq y < 2\}$$

$$(3) X = \mathbf{Z}, \quad Y = \mathbf{N}$$

$$(4) X = [0, 1), \quad Y = [0, \infty) = \{y \mid 0 \leq y\} \quad (\text{hint: 練習問題 2-4(1) 参照})$$

$$(5) X = I = (0, 1), \quad Y = \mathbf{R}$$

$$(6)^* X = [0, 1), \quad Y = \{(x, y) \mid x^2 + y^2 = 1\}$$

### 3 命題と論理

#### 3.1 命題論理学

命題 とは 真 (True) であるか 偽 (False) であるかが定まる文章のことである。疑問文や命令文や感嘆文は命題とは考えられない。

例 次の文章が命題であるか命題でないか考えて見なさい。また命題であれば、その命題が真であるか偽であるか判定しなさい。(あまり、厳密には考えないことにする)

- ・「3 は自然数である」
- ・「 $\frac{3}{5}$  は自然数である」
- ・「鳩山首相は偉大な人である」
- ・「大阪は日本の首都である」
- ・「人間は必ず死ぬ」
- ・「明日は雨が降る」
- ・「昨日風が強かった」
- ・「学校へ行きなさい」
- ・「明石公園の桜はなんときれいなんでしょう」

命題は  $p, q$  などとアルファベットの小文字で表わすことにする。

(1) 否定 (～ではない) (記号  $\neg$ )

$p$  = 「大阪は日本の首都である」

とするとき、

$\neg p$  = 「大阪は日本の首都ではない」

否定の真偽表

| $p$ | $\neg p$ |
|-----|----------|
| T   | F        |
| F   | T        |

(2) 論理和 (=選言 または) (記号  $\vee$ )

$p$  = 「人間は魚類である」

$q$  = 「人間は哺乳類である」

とするとき、

$p \vee q$  = 「人間は魚類であるかまたは人間は哺乳類である」

を表わす。

論理和の真偽表

| $p$ | $q$ | $p \vee q$ |
|-----|-----|------------|
| T   | T   | T          |
| T   | F   | T          |
| F   | T   | T          |
| F   | F   | F          |

(3) 論理積 (=連言 かつ) (記号  $\wedge$ )

$p =$  「クジラは魚類である」

$q =$  「人間は哺乳類である」

とすると、

$p \wedge q =$  「クジラは魚類でありかつ人間は哺乳類である」

を表わす。

論理積の真偽表

| $p$ | $q$ | $p \wedge q$ |
|-----|-----|--------------|
| T   | T   | T            |
| T   | F   | F            |
| F   | T   | F            |
| F   | F   | F            |

(4) 含意 (ならば) (記号  $\Rightarrow$ )

$p =$  「風が吹く」

$q =$  「桶屋が儲かる」

とすると、

$p \Rightarrow q =$  「風が吹けば桶屋が儲かる」

を表わす。

含意の真偽表

| $p$ | $q$ | $p \Rightarrow q$ |
|-----|-----|-------------------|
| T   | T   | T                 |
| T   | F   | F                 |
| F   | T   | T                 |
| F   | F   | T                 |

「 $p \Rightarrow q$ 」は「 $(\neg p) \vee q$ 」と同じであることは次の真偽表から分かる。

| $p$ | $q$ | $\neg p$ | $(\neg p) \vee q$ |
|-----|-----|----------|-------------------|
| T   | T   | F        | T                 |
| T   | F   | F        | F                 |
| F   | T   | T        | T                 |
| F   | F   | T        | T                 |

「 $p \Rightarrow q$ 」の真偽表が納得がいかないかもしれないが、このことは後の定理 4.2 (de Morgan の法則) の後で、触れることにする。

(5) 同値 (記号  $\Leftrightarrow$ )

$p =$  「Aさんは生きている」

$q =$  「Aさんは死んでいない」

とすると、

$p \Leftrightarrow q =$  「Aさんは生きていることとAさんは死んでいないことは同値である」

を表わす。

同値の真偽表

| $p$ | $q$ | $p \Leftrightarrow q$ |
|-----|-----|-----------------------|
| T   | T   | T                     |
| T   | F   | F                     |
| F   | T   | F                     |
| F   | F   | T                     |

いくつかの命題と  $\neg, \vee, \wedge, \Rightarrow, \Leftrightarrow$  を用いて書かれた式を 論理式 という.

$$\text{「}\neg(\neg p)\text{」と「}p\text{」}$$

$$\text{「}p \Rightarrow q\text{」と「}(\neg p) \vee q\text{」}$$

のように, どのような場合でも真偽が等しい論理式を 論理的に同値 であるといい, 次のように記号「 $\equiv$ 」で表わす.

$$\neg(\neg p) \equiv p$$

$$p \Rightarrow q \equiv (\neg p) \vee q$$

次の3つの定理が成り立つ.

### 定理 3.1

$$(1) \quad \neg(\neg p) \equiv p$$

$$(2) \quad p \vee p \equiv p, \quad p \wedge p \equiv p$$

$$(3) \quad p \vee q \equiv q \vee p, \quad p \wedge q \equiv q \wedge p \quad (\text{交換法則})$$

$$(4) \quad (p \vee q) \vee r \equiv p \vee (q \vee r), \quad (p \wedge q) \wedge r \equiv p \wedge (q \wedge r) \quad (\text{結合法則})$$

$$(5) \quad p \wedge (\neg p) \equiv F \quad (\text{矛盾律}), \quad p \vee (\neg p) \equiv T \quad (\text{排中律})$$

$$(6) \quad p \wedge T \equiv p, \quad p \vee T \equiv T$$

$$(7) \quad p \wedge F \equiv F, \quad p \vee F \equiv p$$

### 定理 3.2(de Morgan の法則)

$$(8) \quad \neg(p \vee q) \equiv (\neg p) \wedge (\neg q)$$

$$(9) \quad \neg(p \wedge q) \equiv (\neg p) \vee (\neg q)$$

### 定理 3.3(分配法則)

$$(10) \quad p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$$

$$(11) \quad p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$$

### 含意 $p \Rightarrow q$ の真偽表についての注意

「 $p \Rightarrow q$ 」の否定は「 $p$ であるが $q$ でない」である. すなわち「 $\neg(p \Rightarrow q) \equiv (p \wedge (\neg q))$ 」. この否定を考えると「 $\neg\neg(p \Rightarrow q) \equiv \neg(p \wedge (\neg q))$ 」. これと, de Morgan の法則を用いると「 $p \Rightarrow q \equiv \neg(p \wedge (\neg q)) \equiv (\neg p) \vee q$ 」となる, すなわち「 $p \Rightarrow q$ 」の真偽表と「 $(\neg p) \vee q$ 」の真偽表は同じになる. (これで「 $p \Rightarrow q$ 」の真偽表が納得できたかな?)

逆・対偶・裏

命題「 $p \Rightarrow q$ 」に対して、

「 $q \Rightarrow p$ 」を 逆 ( $q \Rightarrow p \equiv (\neg q) \vee p$ )

「 $(\neg p) \Rightarrow (\neg q)$ 」を 裏 ( $(\neg p) \Rightarrow (\neg q) \equiv p \vee (\neg q)$ )

「 $(\neg q) \Rightarrow (\neg p)$ 」を 対偶 ( $(\neg q) \Rightarrow (\neg p) \equiv q \vee (\neg p)$ )

という。 $p \Rightarrow q \equiv (\neg p) \vee q$  より、

「元の命題」と「対偶」は論理的に同値、

「裏」と「逆」は論理的に同値

であることが分かる。

練習問題 3-1  $p =$  雨が降る ,  $q =$  風が吹く ,  $r =$  雪が降る

とすると、次の命題を  $p, q, r$  で表わせ。

- (1) 雨が降っているがしかし風は吹いていない。
- (2) 雨混じりの風が吹く。
- (3) 風はないが雪が降っている。
- (4) 雨が降って風が吹かないということはない。
- (5) 雨が降らずに風が吹く。
- (6) 少なくとも雨か雪のいずれかが降る。
- (7) 吹雪である。
- (8) 雨と雪が同時に降ることはない。
- (9) 風混じりの雨かまたは吹雪がくる。
- (10) 風が吹くか吹かないかのどちらかである。

練習問題 3-2  $p =$  「金持ちである」,  $q =$  「孤独である」とする。

- (1) 命題： $p \Rightarrow q$  の真偽表を作れ。また、 $p \Rightarrow q$  を言葉で説明せよ。
- (2) 逆： $q \Rightarrow p$  の真偽表を作れ。また、 $q \Rightarrow p$  を言葉で説明せよ。
- (3) 裏： $(\neg p) \Rightarrow (\neg q)$  の真偽表を作れ。また、 $(\neg p) \Rightarrow (\neg q)$  を言葉で説明せよ。
- (4) 対偶： $(\neg q) \Rightarrow (\neg p)$  の真偽表を作れ。また、 $(\neg q) \Rightarrow (\neg p)$  を言葉で説明せよ。

### 3.2 変数を含んだ命題 (命題関数)

「 $x \geq 0$ 」, 「 $x$  は人間である」などのように変数を含んだ命題を考える．変数は複数個ある場合もある．変数を含んだ命題を 命題関数 という．それらを,  $p(x)$  のように表わす．命題関数の場合も前の3つの定理はそのまま成り立つ． $x$  の定義域 (考える範囲) を 対象領域 とよぶことにする．

$p(x)$  = 「 $x$  は有理数である」とするとき,  $p(7)$  = 「7 は有理数である」,  $p(\pi)$  = 「 $\pi$  は有理数である」となる．

#### 全称記号 ( $\forall$ ) と存在記号 ( $\exists$ ) と否定

$p(x)$  に対して,

$$\forall x p(x) = \text{「すべての } x \text{ に対して, } p(x)\text{」}$$

を表わし,

$$\exists x p(x) = \text{「} p(x) \text{ であるような } x \text{ が存在する」} = \text{「ある } x \text{ が存在して } p(x)\text{」}$$

例えば,  $p(x)$  = 「 $x$  は有理数である」とするとき,

$$\forall x p(x) = \text{「すべての } x \text{ は有理数である」}$$

$$\exists x p(x) = \text{「有理数であるような } x \text{ が存在する」}$$

#### 定理 3.4(de Morgan ?)

$$(12) \quad \neg(\forall x p(x)) = \exists x(\neg p(x))$$

$$(13) \quad \neg(\exists x p(x)) = \forall x(\neg p(x))$$

例 (1) 「すべての実数  $x$  に対して  $x^2 \geq 0$ 」の否定を考えてみよう．

$$p(x) = \text{「} x^2 \geq 0 \text{」}$$

とすると,

$$\text{「すべての実数 } x \text{ に対して } x^2 \geq 0 \text{」} = \forall x p(x)$$

その否定は

$$\begin{aligned} \neg(\forall x p(x)) &= \exists x(\neg p(x)) = \text{「ある実数 } x \text{ に対して, } x^2 \not\geq 0 \text{」} \\ &= \text{「} x^2 \not\geq 0 \text{ となる実数 } x \text{ が存在する」} \end{aligned}$$

(2)  $p(x)$  は (1) と同じとすると, 「ある実数  $x$  に対して  $x^2 \geq 0$ 」の否定は

$$\text{「ある実数 } x \text{ に対して } x^2 \geq 0 \text{」} = \exists x p(x)$$

その否定は

$$\neg(\exists x p(x)) = \forall x(\neg p(x)) = \text{「すべての実数 } x \text{ に対して, } x^2 \not\geq 0 \text{」}$$

練習問題 3-3  $p(x) = \text{『}x \text{ は金持ちだ』}$ ,  $q(x) = \text{『}x \text{ は幸せだ』}$  とするとき, 次の命題を  $p(x)$ ,  $q(x)$  を用いて表わせ.

- (1) いくらかの人間は金持ちだ.
- (2) あらゆる人間は幸せだ.
- (3) 金持ちはみな幸せだ.
- (4) 金持ちでないのに幸せな人はいる.
- (5) 金持ちはみな幸せであるとは限らない.

練習問題 3-4  $p(x) = \text{『}x \text{ は天才だ』}$ ,  $q(x) = \text{『}x \text{ は孤独だ』}$  とするとき, 次の命題を  $p(x)$ ,  $q(x)$  を用いて表わせ.

- (1) 天才はいる.
- (2) あらゆる人間は孤独だ.
- (3) すべての天才は孤独である.
- (4) 天才なのに孤独でない人はいる.
- (5) 天才はみな孤独であるとは限らない.

### 3.3 2つ以上の変数を含んだ命題

$p(x, y) = \text{『}x \geq y\text{』}$  とするとき,

$$\begin{aligned}\forall x \forall y p(x, y) &= \forall x (\forall y p(x, y)) = \forall y \forall x p(x, y) = \forall y (\forall x p(x, y)) \\ &= \text{「すべての } x \text{ とすべての } y \text{ に対して } x \geq y \text{ である」}\end{aligned}$$

$$\begin{aligned}\exists x \exists y p(x, y) &= \exists x (\exists y p(x, y)) = \exists y \exists x p(x, y) = \exists y (\exists x p(x, y)) \\ &= \text{「ある } x \text{ とある } y \text{ が存在して } x \geq y \text{ である」}\end{aligned}$$

$$\begin{aligned}\forall x \exists y p(x, y) &= \forall x (\exists y p(x, y)) \\ &= \text{「すべての } x \text{ に対して, ある } y \text{ が存在して } x \geq y \text{ である」} \\ &\quad (\text{このとき, } y \text{ は } x \text{ に関係してよい})\end{aligned}$$

$$\begin{aligned}\exists y \forall x p(x, y) &= \exists y (\forall x p(x, y)) \\ &= \text{「ある } y \text{ が存在して, すべての } x \text{ に対して } x \geq y \text{ である」} \\ &= \text{「『すべての } x \text{ に対して } x \geq y \text{ となる』ような } y \text{ が存在する」} \\ &\quad (\text{このとき, } y \text{ は } x \text{ に関係してはいけない})\end{aligned}$$

練習問題 3-5  $x$  と  $y$  の対象領域をともに,  $Z$ (整数全体) とし,  $p(x, y) = 「x \geq y」$  とするとき, 次の命題は数学的に正しい(真)か, 間違い(偽)であるか調べなさい. また, その理由についても考えなさい.

$$(1) \quad \forall x \forall y p(x, y) \quad (2) \quad \exists x \exists y p(x, y) \quad (3) \quad \forall x \exists y p(x, y) \quad (4) \quad \exists y \forall x p(x, y)$$

$\forall x$  と  $\forall y$  の順番は入れ替えてもよい. 同様に,  $\exists x$  と  $\exists y$  も順番を入れ替えてもよい. しかし,  $\forall x$  と  $\exists y$  の順序は入れ替えることは出来ない.

### 2 つ以上の変数を含んだ命題の否定

否定命題に関する定理 3.4 を用いると,

$$\begin{aligned} \neg(\forall x \forall y p(x, y)) &= \neg(\forall x (\forall y p(x, y))) \\ &= \exists x (\neg(\forall y p(x, y))) = \exists x (\exists y (\neg p(x, y))) = \exists x \exists y (\neg p(x, y)) \end{aligned}$$

となり, ほかの場合も同様に書き換えると,

$$\begin{aligned} \neg(\forall x \forall y p(x, y)) &= \exists x \exists y (\neg p(x, y)) \\ \neg(\exists x \exists y p(x, y)) &= \forall x \forall y (\neg p(x, y)) \\ \neg(\forall x \exists y p(x, y)) &= \exists x \forall y (\neg p(x, y)) \\ \neg(\exists x \forall y p(x, y)) &= \forall x \exists y (\neg p(x, y)) \end{aligned}$$

となる.

否定の記号 ( $\neg$ ) を中へ (右へ) 移動すると, 全称記号 ( $\forall$ ) と存在記号 ( $\exists$ ) が逆になる.

練習問題 3-6 練習問題 3-5 において, (1),(2),(3),(4) の命題の否定命題を作り, それを文章で表しなさい. また, それらは数学的に正しい(真)か, 間違い(偽)であるか調べなさい. また, その理由についても考えなさい.

練習問題 3-7 (2007 年度定期試験問題)  $p(x, n) = 「x < n」$  とおく.  $x$  の対象領域をすべての正の実数とし,  $n$  の対象領域をすべての自然数とする. 次の命題を全称記号 ( $\forall$ ) や存在記号 ( $\exists$ ) と  $p(x, n)$  を用いて表わせ. また, その否定命題を記号と文章の両方で表わしなさい.

『すべての正の実数  $x$  に対して,  $x < n$  となる自然数  $n$  が存在する』

練習問題 3-8 左側の命題が真であるとき，かつその事しか分かっていないとき，右側の命題が真，偽あるいは真偽不明のいずれであるか答えよ．また，その理由についても考えてみなさい．

- (1) 飛ぶ能力のないものは鳥でない．： 鳥のみが飛ぶ能力を持つ．( )
- (2) 飛ぶ能力のない鳥がいる．： あらゆる鳥は飛ぶ能力を持っている．( )

練習問題 3-9 左側の命題がカッコ内に指示された真偽の値を持つとき，かつその事しか分かっていないとき，右側の命題が真，偽あるいは真偽不明のいずれであるか．その理由についても考えてみなさい．

(命題が偽であるのはその否定命題が真であるときである)

- (1) あらゆる天才は怠け者である．(False)： どんな天才も怠け者でない．( )
- (2) 選挙権をもたないものは学生でない．(True)： 学生のみが選挙権を持つ．( )
- (3) あらゆるゾウは水中を泳ぐ．(False)： 水中を泳がないものはゾウでない．( )
- (4) 信仰のない人間がいる．(True)： あらゆる人間は信仰をもっている．( )

練習問題 3-10(保育士採用試験用問題集より)

- 絵が好きな人は旅行が好きである．
- 研究者は健康ではない．
- 旅行が好きな人は健康である．

以上のことから確実にいえるものは，次のうちどれか．

- (1) 研究者は旅行が好きである．
- (2) 研究者は絵が好きではない．
- (3) 健康な人は絵が好きである．
- (4) 旅行が好きな人は絵が好きである．
- (5) 旅行が好きでない人は健康ではない．

練習問題 3-11(保育士採用試験用問題集より)

下のような関係があるとするとき，確実にいえることは次のうちどれか．

- 水泳が好きな人は，陸上が好きである．
  - 水泳が好きではない人は，体操が好きである．
  - 体操が好きな人は，スキーが好きである．
- (1) 陸上が好きでない人は，水泳が好きである．
  - (2) 水泳が好きな人は，体操が好きではない．
  - (3) 体操が好きでない人は，陸上が好きではない．
  - (4) スキーが好きでない人は，陸上が好きである．
  - (5) 水泳が好きでない人は，スキーが好きではない．

## 4 $b$ -進法

### . 10 進法

$$(357.062\cdots)_{10} = 3 \cdot 10^2 + 5 \cdot 10^1 + 7 \cdot 10^0 + 0 \cdot 10^{-1} + 6 \cdot 10^{-2} + 2 \cdot 10^{-3} + \cdots$$

### . 2 進法

$$(357.062\cdots)_2 = 3 \cdot 2^2 + 5 \cdot 2^1 + 7 \cdot 2^0 + 0 \cdot 2^{-1} + 6 \cdot 2^{-2} + 2 \cdot 2^{-3} + \cdots$$

### . $b$ -進法

$$(d_{k-1}d_{k-2}\cdots d_0.d_{-1}d_{-2}\cdots)_b = d_{k-1} \cdot b^{k-1} + d_{k-2} \cdot b^{k-2} + \cdots + d_0 \cdot b^0 + d_{-1} \cdot b^{-1} + d_{-2} \cdot b^{-2} + \cdots$$

$$b : \text{base(基数)} \quad d_i : \text{digit(数字)}$$

$$2 \text{ 進法 (binary system)} \quad \text{bit: binary digit を縮めた言い方} \quad 0 \text{ or } 1$$

$11 \leq b \leq 26$  の時は  $0 \sim 25$  までの数字に  $A \sim Z$  を割り当てる . あるいは

$11 \leq b \leq 36$  の時は  $0 \sim 9$  まではそのまま用い ,  $10 \sim 35$  の数字に  $A \sim Z$  を割り当てる .

コンピュータで 16 進法は

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A(10), B(11), C(12), D(13), E(14), F(15)$$

を用いる .

例 1 (1)  $(11001001)_2 = 1 \cdot 2^7 + 1 \cdot 2^6 + 1 \cdot 2^3 + 1 = 128 + 64 + 8 + 1 = 201$

(2)  $(BAD)_{26} = 1 \cdot 26^2 + 0 \cdot 26^1 + 3 \cdot 26^0 = 676 + 3 = 679$

$$(B.AD)_{26} = 1 \cdot 26^0 + 0 \cdot 26^{-1} + 3 \cdot 26^{-2} = 1 + \frac{3}{676}$$

例 2 160 と 199 を 7 進法で表わし , 7 進法で掛け算せよ .

|                                                                                                                                   |                                                                                                                                   |                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| $\begin{array}{r} 7 \overline{) 160} \cdots 6 \\ 7 \overline{) 22} \cdots 1 \\ 7 \overline{) 3} \cdots 3 \\ \hline 0 \end{array}$ | $\begin{array}{r} 7 \overline{) 199} \cdots 3 \\ 7 \overline{) 28} \cdots 0 \\ 7 \overline{) 4} \cdots 4 \\ \hline 0 \end{array}$ | $\begin{array}{r} (316)_7 \\ \times (403)_7 \\ \hline (1254)_7 \\ (1603)_7 \\ \hline (161554)_7 \end{array}$ |
|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|

$$160 = 7 \times 22 + 6 = 7(7 \times 3 + 1) + 6 = \underline{3} \times 7^2 + \underline{1} \times 7 + \underline{6} = (316)_7$$

$$199 = 7 \times 28 + 3 = 7(7 \times 4 + 0) + 3 = \underline{4} \times 7^2 + \underline{0} \times 7 + \underline{3} = (403)_7$$

$$(316)_7 \times (403)_7 = (161554)_7$$

例 3 12345 を 26 進法 ( $A=0 \sim Z=25$ ) で表わせ .

$$\begin{array}{r} 26 \overline{) 12345} \cdots 21(V) \\ 26 \overline{) 474} \cdots 6(G) \\ 26 \overline{) 18} \cdots 18(S) \\ \hline 0 \end{array}$$

$$12345 = 26 \times 474 + 21 = 26(26 \times 18 + 6) + 6 = \underline{18} \times 26^2 + \underline{6} \times 26 + \underline{21} = (SGV)_{26}$$

例 4  $\pi = 3.1415926 \dots$  を 7 進法で小数点以下 4 桁まで表わせ .

$$\underline{3}.1415926 \dots = \underline{d_0} + d_{-1} \cdot 7^{-1} + d_{-2} \cdot 7^{-2} + d_{-3} \cdot 7^{-3} + d_{-4} \cdot 7^{-4} + \dots$$

$3 = d_0$  , 上の両辺から  $3 = d_0$  を引く .

$$0.1415926 \dots = d_{-1} \cdot 7^{-1} + d_{-2} \cdot 7^{-2} + d_{-3} \cdot 7^{-3} + d_{-4} \cdot 7^{-4} + \dots$$

7 倍する .

$$\underline{0}.991148 \dots = \underline{d_{-1}} + d_{-2} \cdot 7^{-1} + d_{-3} \cdot 7^{-2} + d_{-4} \cdot 7^{-3} + \dots$$

$0 = d_{-1}$  , 両辺から  $0 = d_{-1}$  を引いて 7 倍する .

$$\underline{6}.93804 \dots = \underline{d_{-2}} + d_{-3} \cdot 7^{-1} + d_{-4} \cdot 7^{-2} + \dots$$

$6 = d_{-2}$  , 両辺から  $6 = d_{-2}$  を引いて 7 倍する .

$$\underline{6}.5662 \dots = \underline{d_{-3}} + d_{-4} \cdot 7^{-1} + d_{-5} \cdot 7^{-2} + \dots$$

$6 = d_{-3}$  , 両辺から  $6 = d_{-3}$  を引いて 7 倍する .

$$\underline{3}.963 \dots = \underline{d_{-4}} + d_{-5} \cdot 7^{-1} + d_{-6} \cdot 7^{-2} + \dots$$

$3 = d_{-4}$

以上より  $\pi = 3.1415926 \dots = (3.0663 \dots)_7$

練習問題 4-1 次の数を 10 進法で表わせ .

$$(1) \quad (471)_8 \qquad (2) \quad (11011011)_2 \qquad (3) \quad (165)_7$$

練習問題 4-2 次の問いに答えよ . ただし , 16 進法のときは 10 を A で , 11 を B で , 12 を C で , 13 を D で , 14 を E で , 15 を F とする .

- (1) 1000 を 2 進法で表わせ .                      (2) 1000 を 16 進法で表わせ .  
 (3) 10.25 を 2 進法で表わせ .                      (4) 123.5 を 8 進法で表わせ .

練習問題 4-3 次の 26 進法 ( $A=0 \sim Z=25$ ) で表わされた数を 10 進法で表わせ .

$$(1) \quad (\text{KOBE})_{26} \qquad (2) \quad (\text{YAMA})_{26}$$

練習問題 4-4 次の数を 26 進法 ( $A=0 \sim Z=25$ ) で表わせ .

$$(1) \quad 176332 \qquad (2) \quad 3687172$$

練習問題 4-5 自然対数の底  $e = 2.7182818 \dots$  を 5 進法で小数点以下 4 桁まで表わせ .

## 5 代数の話 (整数の話)

### 5.1 素数の7つの不思議 (朝日新聞 2004/09/14 夕刊より)

#### 話題1 (長い研究の歴史と今も残る難問)

- Fermat の最終定理 (Fermat 予想)

「 $x^n + y^n = z^n$  は  $n \geq 3$  の時, 非自明な (どれも 0 ではない) 整数解は存在しない」  
 の決着=証明 (アンドリュー・ワイルズ=Andrew John Wiles が 1994 年に最終的に証明)  
 に 360 年以上を要した .

$n = 2$  のときの解をピタゴラス数という . ピタゴラス数は無限にある .

$(x, y, z) = (3, 4, 5), (5, 12, 13), \dots$

原始ピタゴラス数 (最大公約数が 1 であるもの) は次の形で求まる .

$$x = |m^2 - n^2|, \quad y = 2mn, \quad z = m^2 + n^2$$

$x$  と  $y$  は入れ替えてよいこととし,  $m, n$  は互いに素で, 一方が偶数とする .

- 完全数

「その数以外の正の約数の和がその数に等しい自然数」

例  $6 = 1 + 2 + 3$  ,  $28 = 1 + 2 + 4 + 7 + 14$

28 からは小さい順に, 496, 8128, 33550336, ... (現在まで 46 個知られている)

偶数の完全数が無数に存在するか、奇数の完全数は存在するか、末尾が 6 か 8 以外の完全数は存在するか、という問題は未解決である。(Wikipedia より)

- 双子素数予想

「差が 2 である素数の組は無限にある」

は未解決 .

例  $(3, 5), (5, 7), (11, 13), \dots$

- Goldbach 予想

「4 以上のすべての偶数は 2 つの素数の和で表わせる」

「6 以上のすべての偶数は 2 つの奇素数の和で表わせる」

は未解決 .

例  $4 = 2 + 2$  ,  $6 = 3 + 3$  ,  $8 = 3 + 5$  ,  $10 = 5 + 5 = 3 + 7$  ,  $12 = 5 + 7$  , ...

#### 話題2 (旧石器時代から素数は知られていた?)

コンゴのイシャンゴ遺跡から見つかった骨には 3 列にわたって数字が刻み込まれているが, その 1 列には

11, 13, 17, 19

と素数ばかり並んでいる . また, 全部で 16 個の数字のうち 10 個が素数  
 (2 万年前の遺跡でメソポタミア文明より 1 万年以上前)

## 話題 3 (まだまだ遠い Riemann 予想の解決)

Riemann 予想

「Riemann のゼータ関数

$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots + \frac{1}{k^s} + \cdots$$

のゼロ点は自明なゼロ点 (負の偶数) を除けばすべて  $\operatorname{Re}(s) = \frac{1}{2}$  のところにある」  
 の解決はまだまだ時間を要しそう。

## 話題 4 (自然数の中に素数はどれくらいある? = 素数分布)

 $\pi(x) = x$  以下の素数の個数

$$\pi(10) = 4 \quad (2, 3, 5, 7)$$

$$\pi(100) = 25, \quad \pi(1000) = 168, \quad \pi(10000) = 1229$$

$$\pi(100000) = 9592, \quad \pi(1000000) = 78498$$

$$\pi(10000000) = 664579, \quad \pi(4 \times 10^{22}) = 7.83964159847056303858 \times 10^{20}$$

$$\pi(x) \sim \frac{x}{\log x} \quad \left( \lim_{x \rightarrow \infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1 \right)$$

## 話題 5 (これまでに見つかった最大の素数)

$$2^{24036583} - 1 : 723 \text{ 万 } 5733 \text{ 桁の素数}$$

(現在=2008 年 8 月時点では  $2^{43112609} - 1 \div 3.1647 \times 10^{12978188} : 1297 \text{ 万 } 8189 \text{ 桁の素数}$ )

$2^n - 1$  の形の数をメルセンヌ (Mersenne) 数, それが素数である時はメルセンヌ素数  
 メルセンヌ数は素数かどうか判定しやすい。

一般に大きな数が素数かどうか判定する事より, 大きな数の素因数分解はずっと難しい。

## 話題 6 (10 億桁の素数を見つけると 3 千万円の賞金)

大きな素数は暗号に利用される。

より安全な暗号のためにはより大きな素数の発見が有用。

電子フロンティア財団 (EFF) が素数に賞金

1000 万桁の素数...10 万ドル (約 1000 万円)

1 億桁の素数...15 万ドル (約 1500 万円)

10 億桁の素数...25 万ドル (約 2500 万円)

## 話題 7 (素数は数学の原子)

素数について調べる事は手触り感覚で味わえるので, プロでなくても可能。

数学のプロにとっても奥が深い。数学のいろんなところに広がりをもつ。

## 5.2 整除性と Euclid の互除法

定義  $a, b$ : 整数 (integer) とする .

「 $a$  は  $b$  の約数 (diviser) である」 あるいは  $b$  は  $a$  の倍数 (multiple) である」

$\stackrel{\text{def}}{\iff}$

$\exists d : \text{整数} \quad s.t. \quad b = a \times d$

真の約数 (proper diviser) : 自分自身以外の約数

非自明な約数 (non-trivial diviser) : 自分自身と 1 以外の約数

素数 (prime number) : 2 以上の整数で, 1 と自分自身以外に正の約数をもたないもの

合成数 (composite number) : 少なくとも 1 つの非自明な約数を持つ整数

### 整除性の基本的性質

1.  $b$  が  $a$  の倍数,  $c$  は任意の整数  $\implies b \times c$  は  $a$  の倍数
2.  $b$  が  $a$  の倍数 かつ  $c$  が  $b$  の倍数  $\implies c$  は  $a$  の倍数
3.  $b$  と  $c$  が  $a$  の倍数  $\implies (b \pm c)$  も  $a$  の倍数

### 算術の基本定理 (The Fundamental Theorem of Arithmetic)

任意の自然数は (因子の順序を無視すれば) 一通りに素因数分解が出来る . 小さい素数の順番に書くのが通常である .

(例  $4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7$ )

### 整除性の基本的性質 (続き)

4.  $p$  : 素数,  $b \times c : p$  の倍数  $\implies b : p$  の倍数 または  $c : p$  の倍数
5.  $a : m$  の倍数,  $a : n$  の倍数  
 $m$  と  $n$  が 1 以外の共通の約数 (公約数) をもたない  
 $\implies$   
 $a : m \times n$  の倍数

自然数  $n$  の約数は何通りあるか?

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \text{ (素因数分解)}$$

とすると,  $n$  の任意の約数  $d$  は

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r} \quad (0 \leq \beta_i \leq \alpha_i)$$

の形である . よって,  $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$  の約数の個数は

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1)$$

である .

(例  $4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7$  の約数の個数は  $(3+1)(1+1)(2+1)(1+1) = 48$  個)

定義 0 と異なる 2 つの整数  $a$  と  $b$  について ,  $a$  と  $b$  の両方の約数になっているものを 公約数 (common divider) といい , その最大のものを 最大公約数 (greatest common divider) といい ,  $\underline{g.c.d.(a, b)}$  と書く .

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$$

とすると ,

$$\underline{g.c.d.(a, b)} = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_r^{\gamma_r} \quad \text{ここで , } \gamma_i = \min(\alpha_i, \beta_i)$$

$a$  と  $b$  の両方の倍数になっているものを 公倍数 (common multiple) といい , その最小のものを 最小公倍数 (least common multiple) といい ,  $\underline{l.c.m.(a, b)}$  と書く .

$$\underline{l.c.m.(a, b)} = p_1^{\delta_1} p_2^{\delta_2} \cdots p_r^{\delta_r} \quad \text{ここで , } \delta_i = \max(\alpha_i, \beta_i)$$

$$\underline{l.c.m.(a, b)} = \frac{|a \cdot b|}{\underline{g.c.d.(a, b)}} \quad (\max(\alpha, \beta) + \min(\alpha, \beta) = \alpha + \beta)$$

例  $4200 = 2^3 \cdot 3^1 \cdot 5^2 \cdot 7^1$  ,  $10780 = 2^2 \cdot 5^1 \cdot 7^2$

$$\underline{g.c.d.(4200, 10780)} = 2^2 \cdot 5^1 \cdot 7^1$$

$$\underline{l.c.m.(4200, 10780)} = 2^3 \cdot 3^1 \cdot 5^2 \cdot 7^2$$

### Euclid の互除法 (Euclidean algorithm)

大きな数に対して素因数分解が分からない時でも , 2 つの数  $a$  と  $b$  の最大公約数  $\underline{g.c.d.(a, b)}$  を簡単な方法で求める事が出来る .

#### 原理

$a \geq b$  とする .  $a \div b$  : 商を  $q$  , 余りを  $r$  とする . すなわち ,  $a = bq + r$  ( $0 \leq r \leq b-1$ )

このとき ,  $\underline{g.c.d.(a, b)} = \underline{g.c.d.(b, r)}$  ( $\because d : a$  と  $b$  の公約数  $\iff d : b$  と  $r$  の公約数)

#### algorithm

$a \geq b$  とする .

- |     |                                               |                      |                                                               |
|-----|-----------------------------------------------|----------------------|---------------------------------------------------------------|
| (1) | $a \div b$ : 商 $q_1$ , 余り $r_1 (r_1 > 0)$     | $a = bq_1 + r_1$     | $\underline{g.c.d.(a, b)} = \underline{g.c.d.(b, r_1)}$       |
| (2) | $b \div r_1$ : 商 $q_2$ , 余り $r_2 (r_2 > 0)$   | $b = r_1q_2 + r_2$   | $\underline{g.c.d.(b, r_1)} = \underline{g.c.d.(r_1, r_2)}$   |
| (3) | $r_1 \div r_2$ : 商 $q_3$ , 余り $r_3 (r_3 > 0)$ | $r_1 = r_2q_3 + r_3$ | $\underline{g.c.d.(r_1, r_2)} = \underline{g.c.d.(r_2, r_3)}$ |

.....

- |     |                                                       |                              |                                                                           |
|-----|-------------------------------------------------------|------------------------------|---------------------------------------------------------------------------|
| (k) | $r_{k-2} \div r_{k-1}$ : 商 $q_k$ , 余り $r_k (r_k > 0)$ | $r_{k-2} = r_{k-1}q_k + r_k$ |                                                                           |
|     |                                                       |                              | $\underline{g.c.d.(r_{k-2}, r_{k-1})} = \underline{g.c.d.(r_{k-1}, r_k)}$ |

$$(k+1) \quad r_{k-1} \div r_k : \text{商 } q_{k+1}, \text{ 余り } r_{k+1} = 0 \quad r_{k-1} = r_k q_{k+1} \\ r_k = g.c.d.(r_{k-1}, r_k) = g.c.d.(a, b) : \text{最大公約数}$$

例 1  $g.c.d.(1547, 560)$  を見つけよ .

$$1547 = 560 \cdot 2 + 427$$

$$560 = 427 \cdot 1 + 133$$

$$427 = 133 \cdot 3 + 28$$

$$133 = 28 \cdot 4 + 21$$

$$28 = 21 \cdot 1 + 7$$

$$21 = 7 \cdot 3$$

$$g.c.d.(1547, 560) = 7$$

定理 6.1  $d = g.c.d.(a, b) \implies \exists u, v : \text{整数 } s.t. \ d = au + bv$

すなわち, 2 つの整数  $a$  と  $b$  の最大公約数  $d$  は  $a$  と  $b$  の整数係数の 1 次結合で表わせる .

[証明の概略](以下の方法を 拡張 Euclid の互除法 という) Euclid の互除法の式を逆にたどって,

$d = r_k = r_{k-2} - r_{k-1}q_k$  の式に  $r_{k-1} = r_{k-3} - r_{k-2}q_{k-1}$  を代入 . それに,  $r_{k-2}, r_{k-3}, \dots$  を次々に代入していけば,  $d$  は  $a$  と  $b$  の整数係数の 1 次結合表わせる .

$$\begin{aligned} d = r_k &= \underline{r_{k-2}} - \underline{r_{k-1}}q_k \\ &= \underline{r_{k-2}} - (\underline{r_{k-3}} - \underline{r_{k-2}}q_{k-1})q_k = \underline{r_{k-2}}(1 + q_{k-1}q_k) - \underline{r_{k-3}}q_k \\ &= (\underline{r_{k-4}} - \underline{r_{k-3}}q_{k-2})(1 + q_{k-1}q_k) - \underline{r_{k-3}}q_k = \underline{r_{k-4}}(1 + q_{k-1}q_k) - \underline{r_{k-3}}(q_{k-2} + q_k + q_kq_{k-1}q_{k-2}) \\ &= \underline{r_{k-4}}(1 + q_{k-1}q_k) - (\underline{r_{k-5}} - \underline{r_{k-4}}q_{k-3})(q_{k-2} + q_k + q_kq_{k-1}q_{k-2}) = \dots \\ &= \dots \end{aligned}$$

例 1(続き)

$$\begin{aligned} 7 &= 28 - 21 \cdot 1 = 28 - (133 - 28 \cdot 4) \cdot 1 \\ &= 5 \cdot 28 - 1 \cdot 133 = 5 \cdot (427 - 133 \cdot 3) - 1 \cdot 133 \\ &= 5 \cdot 427 - 16 \cdot 133 = 5 \cdot 427 - 16 \cdot (560 - 427 \cdot 1) \\ &= 21 \cdot 427 - 16 \cdot 560 = 21 \cdot (1547 - 560 \cdot 2) - 16 \cdot 560 \\ &= 21 \cdot 1547 - 58 \cdot 560 \end{aligned}$$

定義  $a, b$ : 整数 (integer) とする .

$a$  と  $b$  は互いに素 (relatively prime)

$\stackrel{\text{def}}{\iff}$

$g.c.d.(a, b) = 1$  (i.e.  $a$  と  $b$  は 1 より大きな公約数を持たない)

定義 (Euler の  $\varphi$  関数)

$n$ : 自然数 (natural number) とする .

$$\varphi(n) \stackrel{\text{def}}{=} \# \{b \in \mathbb{Z} \mid 1 \leq b \leq n \text{ かつ } g.c.d.(b, n) = 1\}$$

( $\#$  は集合の個数を表わすこと事にする)

$\varphi(n)$  は  $n$  以下の  $n$  と互いに素である数の個数である .

例  $\varphi(1) = \# \{1\} = 1$  ,  $\varphi(2) = \# \{1\} = 1$  ,  $\varphi(3) = \# \{1, 2\} = 2$  ,  
 $\varphi(4) = \# \{1, 3\} = 2$  ,  $\varphi(5) = \# \{1, 2, 3, 4\} = 4$  ,  $\varphi(6) = \# \{1, 5\} = 2$

$p$ : 素数のとき ,  $\varphi(p) = \# \{1, 2, \dots, p-1\} = p-1$

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right)$$

( $\because$   $1 \sim p^\alpha$  のうち ,  $p^\alpha$  と素でないものは  $\{1 \cdot p, 2 \cdot p, \dots, p^{\alpha-1} \cdot p\}$  の  $p^{\alpha-1}$  個)

練習問題 6-1 945 の約数は何個あるか? それらをすべて挙げよ .

練習問題 6-2 (1)  $n!$  の約数になっている素数  $p$  の巾 ( $p^k$ ) の中で最大の  $k$  は

$$\left[ \frac{n}{p} \right] + \left[ \frac{n}{p^2} \right] + \left[ \frac{n}{p^3} \right] + \dots \quad (\text{有限和})$$

であることを示せ .

(2)  $100!$  は 2 の何乗で割り切れるか?

$100!$  は 3 の何乗で割り切れるか?

$100!$  は 5 の何乗で割り切れるか?

$100!$  は 7 の何乗で割り切れるか?

$100!$  を素因数分解せよ .

練習問題 6-3  $d = g.c.d.(360, 294)$  を 2 つの方法で求めよ .

(1) 2 つの数を素因数分解して求める方法

(2) Euclid の互除法

練習問題 6-4 つぎの 2 つの数の最大公約数を Euclid の互除法を用いて求め , その最大公約数を 2 つの数の 1 次結合で表わせ .

(1) 26 , 18      (2) 187 , 34      (3) 841 , 160      (4) 2613 , 2171

練習問題 6-5 次の自然数  $n$  について , Euler の  $\varphi$  関数  $\varphi(n)$  を求めなさい ,

(1)  $n = 12$       (2)  $n = 20$       (3)  $n = 40$       (4)  $n = 100$

### 5.3 合同式

#### 定義

$a \equiv b \pmod{m} \stackrel{\text{def}}{\iff} (a - b) \text{ が } m \text{ の倍数}$

このとき,  $m$  を法として  $a$  と  $b$  は合同である という.

#### 合同式の基本的性質

- $a \equiv a \pmod{m}$
  - $a \equiv b \pmod{m} \iff b \equiv a \pmod{m}$
  - $a \equiv b \pmod{m}$  かつ  $b \equiv c \pmod{m} \implies a \equiv c \pmod{m}$

(i) ~ (iii) をみたす関係  $\equiv$  を 同値関係 という.
- 集合に同値関係があるとき, 同じ関係をもつものを集めたものを 同値類 という.  
いまの場合,  $m$  で割った余りが同じであるものを集めたものであるので, これを  $m$  を法とする剰余類 といい,  $\mathbb{Z}/m\mathbb{Z}$  で表わす.  $\mathbb{Z}/m\mathbb{Z}$  は

0 と合同な同値類  $\{\dots, -2m, -m, 0, m, 2m, 3m, \dots\}$

1 と合同な同値類  $\{\dots, -2m+1, -m+1, 1, m+1, 2m+1, 3m+1, \dots\}$

2 と合同な同値類  $\{\dots, -2m+2, -m+2, 2, m+2, 2m+2, 3m+2, \dots\}$

.....

$(m-1)$  と合同な同値類  $\{\dots, -2m-1, -m-1, -1, m-1, 2m-1, \dots\}$

の  $m$  個の同値類が出来る.

- $a \equiv b \pmod{m}$  かつ  $c \equiv d \pmod{m}$   
 $\implies (a \pm c) \equiv (b \pm d) \pmod{m}$  かつ  $ac \equiv bd \pmod{m}$
- $d$  が  $m$  の約数であるとき,  $a \equiv b \pmod{m} \implies a \equiv b \pmod{d}$
- $m$  と  $n$  が互いに素であるとき ( $\text{g.c.d.}(m, n) = 1$ )  
 $a \equiv b \pmod{m}, a \equiv b \pmod{n} \implies a \equiv b \pmod{m \cdot n}$

**定理 6.2**  $\mathbb{Z}/m\mathbb{Z}$  において,

$a$  が掛け算の逆元  $b = a^{-1}$  (i.e.  $a \cdot b \equiv a \cdot a^{-1} \equiv 1 \pmod{m}$ ) をもつ

$\iff$

$\text{g.c.d.}(a, m) = 1$

**proof**  $\implies$  の証明

背理法  $\text{g.c.d.}(a, m) = d > 1$  とする.

$ab - 1$  は  $m$  の倍数  $\implies ab - 1$  は  $d$  の倍数  $\implies 1$  は  $d$  の倍数 (矛盾)

$\Leftarrow$  の証明

$\text{g.c.d.}(a, m) = 1$  とすると,  $ua + vm = 1$  となる  $u, v$  がある ( $u, v \in \mathbb{Z}$ ).

$u = b$  とおくと,  $ab - 1 = -vm$  より,  $ab \equiv 1 \pmod{m}$  である.

**Remark**  $\gcd(a, m) = 1$  ,  $ab \equiv 1 \pmod{m}$  とするとき,  $a^{-n}$  で  $b^n \equiv (a^{-1})^n$  の剰余類を表わす.

**例 2** 841 を法とする 160 の逆元  $160^{-1}$  を見つけよ.

問題 6-4(3) より,

$$841 = 160 \cdot 5 + 41$$

$$160 = 41 \cdot 3 + 37$$

$$41 = 37 \cdot 1 + 4$$

$$37 = 4 \cdot 9 + 1$$

$$4 = 1 \cdot 4 + 0$$

より,

$$\begin{aligned} 1 &= 37 - 4 \cdot 9 = 37 - (41 - 37 \cdot 1) \cdot 9 \\ &= 37 \cdot 10 - 41 \cdot 9 = (160 - 41 \cdot 3) \cdot 10 - 41 \cdot 9 \\ &= 160 \cdot 10 - 41 \cdot 39 = 160 \cdot 10 - (841 - 160 \cdot 5) \cdot 39 \\ &= 160 \cdot 205 - 841 \cdot 39 \end{aligned}$$

以上より,  $160 \cdot 205 \equiv 1 \pmod{841}$  すなわち,  $160^{-1} \equiv 205 \pmod{841}$

### 定理 6.3

$a \equiv b \pmod{m}$   $\gcd(a, m) = 1 (\implies \gcd(b, m) = 1)$  とすると,

$$a^{-1} \equiv b^{-1} \pmod{m}$$

が成り立つ.

**proof**

$a \equiv b \pmod{m}$  である. この両辺に  $a^{-1}b^{-1}$  を掛けると,  $a^{-1}b^{-1}a \equiv a^{-1}b^{-1}b \pmod{m}$  より,  $b^{-1} \equiv a^{-1} \pmod{m}$  が成り立つ.

定理 6.4  $0 \leq a, b < m$  のとき, 一次合同方程式

$$ax \equiv b \pmod{m}$$

について考える.

(1)  $g.c.d.(a, m) = 1$  のとき, ある解  $x_0$  が存在し, すべての解  $x$  は  $x = x_0 + mn$  の形である.

(2)  $g.c.d.(a, m) = d > 1$  のとき,  $b$  が  $d$  の倍数であるときのみ解をもち,

$$a = a'd, \quad b = b'd, \quad m = m'd$$

とすると,  $g.c.d.(a', m') = 1$  となり,

$$ax \equiv b \pmod{m} \Leftrightarrow a'x \equiv b' \pmod{m'}$$

定理 6.5 (Fermat の小定理)  $p$  を素数とし,  $a$  を任意の整数とすると,

$$a^p \equiv a \pmod{p}$$

が成り立つ, さらに,  $a$  が  $p$  の倍数でなければ,

$$a^{p-1} \equiv 1 \pmod{p}$$

が成り立つ,

proof

$a$  が  $p$  の倍数でないとする.

$$0 \cdot a, \quad 1 \cdot a, \quad 2 \cdot a, \quad \dots, \quad (p-1) \cdot a$$

はすべて異なる剰余類に属する [なぜなら,  $i \cdot a \equiv j \cdot a \pmod{p}$  ( $0 \leq i, j \leq p-1$ ) とすると,  $(i-j) \cdot a$  は  $p$  の倍数となり,  $a$  は  $p$  と互いに素であることから,  $(i-j)$  が  $p$  の倍数となり,  $0 \leq i, j \leq p-1$  より,  $i = j$  でなければならない.]

$\{1 \cdot a, 2 \cdot a, 3 \cdot a, \dots, (p-1) \cdot a\}$  を並べ替えると,  $p$  を法として,  $\{1, 2, 3, \dots, (p-1)\}$  と等しい. このことから,

$$(1 \cdot a) \cdot (2 \cdot a) \cdot (3 \cdot a) \cdots ((p-1) \cdot a) \equiv (p-1)! \pmod{p}$$

$$(p-1)! \cdot a^{p-1} \equiv (p-1)! \pmod{p}$$

$(p-1)!$  は  $p$  と互いに素であるので,

$$a^{p-1} \equiv 1 \pmod{p}$$

となる. この両辺に  $a$  をかければ,  $a^p \equiv a \pmod{p}$  が得られ, これは  $a$  が  $p$  の倍数のときも成り立つ.

定理 6.5 の系  $p$  を素数とし,  $a$  を  $p$  の倍数でないとする. また,

$$n \equiv m \pmod{p-1}$$

とすると,

$$a^n \equiv a^m \pmod{p}$$

が成り立つ.

**proof**  $n \equiv m \pmod{p-1}$  であることより,  $n = m + c(p-1)$  と書ける.

$$a^n = a^m \cdot (a^{p-1})^c \equiv a^m \pmod{p} \quad (\because a^{p-1} \equiv 1 \pmod{p})$$

**例 3**  $2^{1000000}$  を 7 進法で表示するとき, 第 1 位の数字は何か? ( $2^{1000000}$  を 7 で割った余りを求めよ)

$$p = 7 \text{ とすると, } 1000000 \div (7-1) = 166666 \cdots 4 \quad i.e. \quad 1000000 = 6 \times 166666 + 4$$

$$1000000 \equiv 4 \pmod{7-1} \text{ より, } 2^{1000000} \equiv 2^4 \equiv 2 \pmod{7}$$

**定理 6.6(中国剰余定理=Chinese Remainder Theorem)**

連立合同方程式

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots\dots\dots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

を考える

$i \neq j$  のとき  $\text{g.c.d.}(m_i, m_j) = 1$  (どの異なる  $m_i$  と  $m_j$  も互いに素) をみたせば,  $M = m_1 m_2 \cdots m_r$  を法として一意に解は存在する.

**proof**

$M$  を法として解は一意的であることの証明

$x'$  と  $x''$  を 2 つの解とする.

すべての  $i$  について,

$$x = x' - x'' \equiv 0 \pmod{m_i}$$

どの  $m_i$  も互いに素であるので, 合同式の基本的性質 5 より,

$$x = x' - x'' \equiv 0 \pmod{M = m_1 m_2 \cdots m_r}$$

解の存在証明

$M_i = M/m_i$  とおく.  $\text{g.c.d.}(M_i, m_i) = 1$  より,  $\exists N_i \text{ s.t. } N_i M_i \equiv 1 \pmod{m_i}$

$$x = \sum_{j=1}^r a_j M_j N_j$$

$i \neq j$  のとき,  $M_i$  は  $m_i$  の倍数になっており,  $M_i N_i \equiv 1 \pmod{m_i}$  より,

$$x \equiv a_i M_i N_i \equiv a_i \pmod{m_i}$$

## 例 4 連立合同方程式

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

上の解の存在証明に当てはめて解こう.

$$M = 3 \times 5 \times 7 = 105, \quad M_1 = M/3 = 35, \quad M_2 = M/5 = 21, \quad M_3 = M/7 = 15$$

$$35 \times 2 = 70 \equiv 1 \pmod{3} \text{ より, } N_1 \equiv M_1^{-1} \equiv 2 \pmod{3}$$

$$21 \times 1 = 21 \equiv 1 \pmod{5} \text{ より, } N_2 \equiv M_2^{-1} \equiv 1 \pmod{5}$$

$$15 \times 1 = 15 \equiv 1 \pmod{7} \text{ より, } N_3 \equiv M_3^{-1} \equiv 1 \pmod{7}$$

$$\text{以上より, } x \equiv 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 = 233 \equiv 23 \pmod{105}$$

## 定理 6.6 の系

$$m \text{ と } n \text{ が互いに素 } (g.c.d.(m, n) = 1) \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$$

proof(講義では省略)

$$0 \sim (mn - 1) \text{ に } mn \text{ と互いに素な数が何個あるか? } \varphi(mn)$$

$$0 \leq \forall j \leq (mn - 1) \quad j_1 : j \text{ を } m \text{ で割ったときの余り}$$

$$j_2 : j \text{ を } n \text{ で割ったときの余り}$$

定理 6.6(中国剰余定理) より,  $j$  と  $(j_1, j_2)$  は 1 対 1 に対応する.

$$(\because \exists! j \text{ s.t. } j \equiv j_1 \pmod{m} \text{ かつ } j \equiv j_2 \pmod{n})$$

また,

$$j \text{ と } mn \text{ と互いに素} \iff j_1 \text{ が } m \text{ と互いに素 かつ } j_2 \text{ が } n \text{ と互いに素}$$

以上より,

$$\begin{aligned} \varphi(mn) &= (mn \text{ と互いに素な } j \text{ の個数}) \\ &= (m \text{ と互いに素な } j_1 \text{ の個数}) \times (n \text{ と互いに素な } j_2 \text{ の個数}) \\ &= \varphi(m)\varphi(n) \end{aligned}$$

この定理 6.6 の系を用いると, 素因数分解された  $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$  とすると,

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}) \\ &= \varphi(p_1^{\alpha_1}) \varphi(p_2^{\alpha_2}) \cdots \varphi(p_r^{\alpha_r}) \\ &= p_1^{\alpha_1} \left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2} \left(1 - \frac{1}{p_2}\right) \cdots p_r^{\alpha_r} \left(1 - \frac{1}{p_r}\right) \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right) \\ \varphi(n) &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right) = n \times \prod_{p|n: \text{素数}} \left(1 - \frac{1}{p}\right) \end{aligned}$$

例  $\varphi(12) = 12 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 4$  ,  $\varphi(100) = 100 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) = 40$

定理 6.7(Euler)  $a$  が  $m$  と素 ( $\gcd(a, m) = 1$ ) であるとき,

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

が成り立つ.

proof(講義では省略)

(i)  $m = p^\alpha$  ( $p$ : 素数) のとき,  $\alpha$  に関する帰納法で証明する.

$$\alpha = 1 \text{ のとき, } a^{\varphi(m)} = a^{\varphi(p)} = a^{p-1} \equiv 1 \pmod{p = m}$$

$$\alpha = k \text{ のとき, 成り立つと仮定すると } a^{\varphi(p^k)} = a^{p^k - p^{k-1}} \equiv 1 \pmod{p^k}$$

$$\alpha = k + 1 \text{ のときは } a^{\varphi(p^{k+1})} = a^{p^{k+1} - p^k} = a^{p(p^k - p^{k-1})} = \left(a^{p^k - p^{k-1}}\right)^p$$

帰納法の仮定より,  $a^{p^k - p^{k-1}} = 1 + b \cdot p^k$  と書け,

$$a^{\varphi(p^{k+1})} = (1 + b \cdot p^k)^p = {}_p C_0 + {}_p C_1 b \cdot p^k + {}_p C_2 (b \cdot p^k)^2 + \cdots + {}_p C_p (b \cdot p^k)^p$$

この右辺の第 1 項目を除けばすべての項は  $p^{k+1}$  で割り切れるので,

$$a^{\varphi(p^{k+1})} \equiv {}_p C_0 = 1 \pmod{p^{k+1}}$$

(ii)  $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$  のとき, 任意の  $i$  について,

$$a^{\varphi(m)} = a^{\varphi(p_1^{\alpha_1}) \varphi(p_2^{\alpha_2}) \cdots \varphi(p_r^{\alpha_r})} \equiv 1 \pmod{p_i^{\alpha_i}} \quad (\because a^{\varphi(p_i^{\alpha_i})} \equiv 1 \pmod{p_i^{\alpha_i}})$$

合同式の基本的性質 5 より,

$$a^{\varphi(m)} \equiv 1 \pmod{m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}}$$

が成り立つ.

定理 6.7 の系

$a$  と  $m$  が互いに素 ( $\gcd(a, m) = 1$ ) とし,  $n$  を  $\varphi(m)$  で割った余りを  $n'$  とするとき,

$$a^n \equiv a^{n'} \pmod{m}$$

が成り立つ.

proof  $n = n' + c \cdot \varphi(m)$  と書けるので,

$$a^n = a^{n'} \cdot \left(a^{\varphi(m)}\right)^c \equiv a^{n'} \pmod{m} \quad (\because a^{\varphi(m)} \equiv 1 \pmod{m})$$

Remark

$a$  と  $m$  が互いに素であるとき,  $a^{\varphi(m)} \equiv 1 \pmod{m}$  であるが,  $a^x \equiv 1 \pmod{m}$  となるもっと小さな  $x$  を見つけたい.

定理 6.7(Euler) の証明から,  $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$  のとき,  $x$  として,

$\varphi(p_1^{\alpha_1}), \varphi(p_2^{\alpha_2}), \dots, \varphi(p_r^{\alpha_r})$  の最小公倍数をとれば,  $a^x \equiv 1 \pmod{m}$  となる.

例 5  $m = 105 = 3 \cdot 5 \cdot 7$ ,  $a$  を  $m$  と互いに素であるとすれば,  $\varphi(3) = 2$ ,  $\varphi(5) = 4$ ,  $\varphi(7) = 6$  の最小公倍数 12 をとれば,  $a^{12} \equiv 1 \pmod{105}$  ( $\varphi(105) = 2 \cdot 4 \cdot 6 = 48$ )

例 6  $2^{1000000} \equiv ? \pmod{77}$

解法 1(上の Remark を用いる方法)

$77 = 7 \cdot 11$  , ,  $\varphi(7) = 6$  ,  $\varphi(11) = 10$  , 6 と 10 の最小公倍数は 30

$$2^{30} \equiv 1 \pmod{77} , 1000000 = 30 \cdot 33333 + 10$$

$$2^{1000000} = (2^{30})^{33333} \cdot 2^{10} \equiv 2^{10} = 1024 = 77 \cdot 13 + 23 \equiv 23 \pmod{77}$$

解法 2(定理 6.5 の系と定理 6.6(中国剰余定理) を用いる方法)

$$2^{1000000} \equiv ? \pmod{7}$$

$$1000000 = (7 - 1) \cdot 166666 + 4 \text{ より , } 2^{1000000} \equiv 2^4 = 16 \equiv 2 \pmod{7}$$

$$2^{1000000} \equiv ? \pmod{11}$$

$$1000000 = (11 - 1) \cdot 100000 + 0 \text{ より , } 2^{1000000} \equiv 2^0 \equiv 1 \pmod{11}$$

$$x = 2^{1000000} \equiv 2 \pmod{7} , x \equiv 1 \pmod{11} , \text{中国剰余定理の証明と ,}$$

$$11^{-1} \equiv 2 \pmod{7} , 7^{-1} \equiv 8 \pmod{11} \text{ より ,}$$

$$x = 2^{1000000} \equiv 2 \cdot 2 \cdot 11 + 1 \cdot 8 \cdot 7 = 100 \equiv 23 \pmod{77}$$

**問題 6-6** 次の解を求めよ .

- |                                |                                  |
|--------------------------------|----------------------------------|
| (1) $3x \equiv 4 \pmod{7}$     | (2) $3x \equiv 4 \pmod{12}$      |
| (3) $9x \equiv 12 \pmod{21}$   | (4) $27x \equiv 25 \pmod{256}$   |
| (5) $27x \equiv 72 \pmod{900}$ | (6) $103x \equiv 612 \pmod{676}$ |

**問題 6-7** 完全平方数を 16 進法で表わすとき , 第 1 位の数字は何になるか ? 可能な数字をすべてあげよ .

**問題 6-8** 連続する 2 つの正の奇数の積を 12 進法で表わすとき , 第 1 位の数字は何になるか ? 可能な数字をすべてあげよ .

**問題 6-9**  $n$  を 10 進法で表わすとき , 次のことを証明せよ .

$$n \text{ が } 3 \text{ の倍数} \Leftrightarrow (n \text{ の各桁の数字の和}) \text{ が } 3 \text{ の倍数}$$

$$n \text{ が } 9 \text{ の倍数} \Leftrightarrow (n \text{ の各桁の数字の和}) \text{ が } 9 \text{ の倍数}$$

**問題 6-10**  $(n^5 - n)$  は 30 の倍数であることを証明せよ .

問題 6-11 次の連立合同方程式の解を求めよ .

$$(1) \begin{cases} x \equiv 4 \pmod{7} \\ x \equiv 4 \pmod{9} \\ x \equiv 4 \pmod{11} \end{cases}$$

$$(2) \begin{cases} x \equiv 1 \pmod{11} \\ x \equiv 2 \pmod{12} \\ x \equiv 3 \pmod{13} \end{cases}$$

$$(3) \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{11} \\ x \equiv 5 \pmod{16} \end{cases}$$

問題 6-12  $\varphi(90)$  ,  $\varphi(91)$  ,  $\varphi(92)$  ,  $\dots$  ,  $\varphi(100)$  を求めよ .