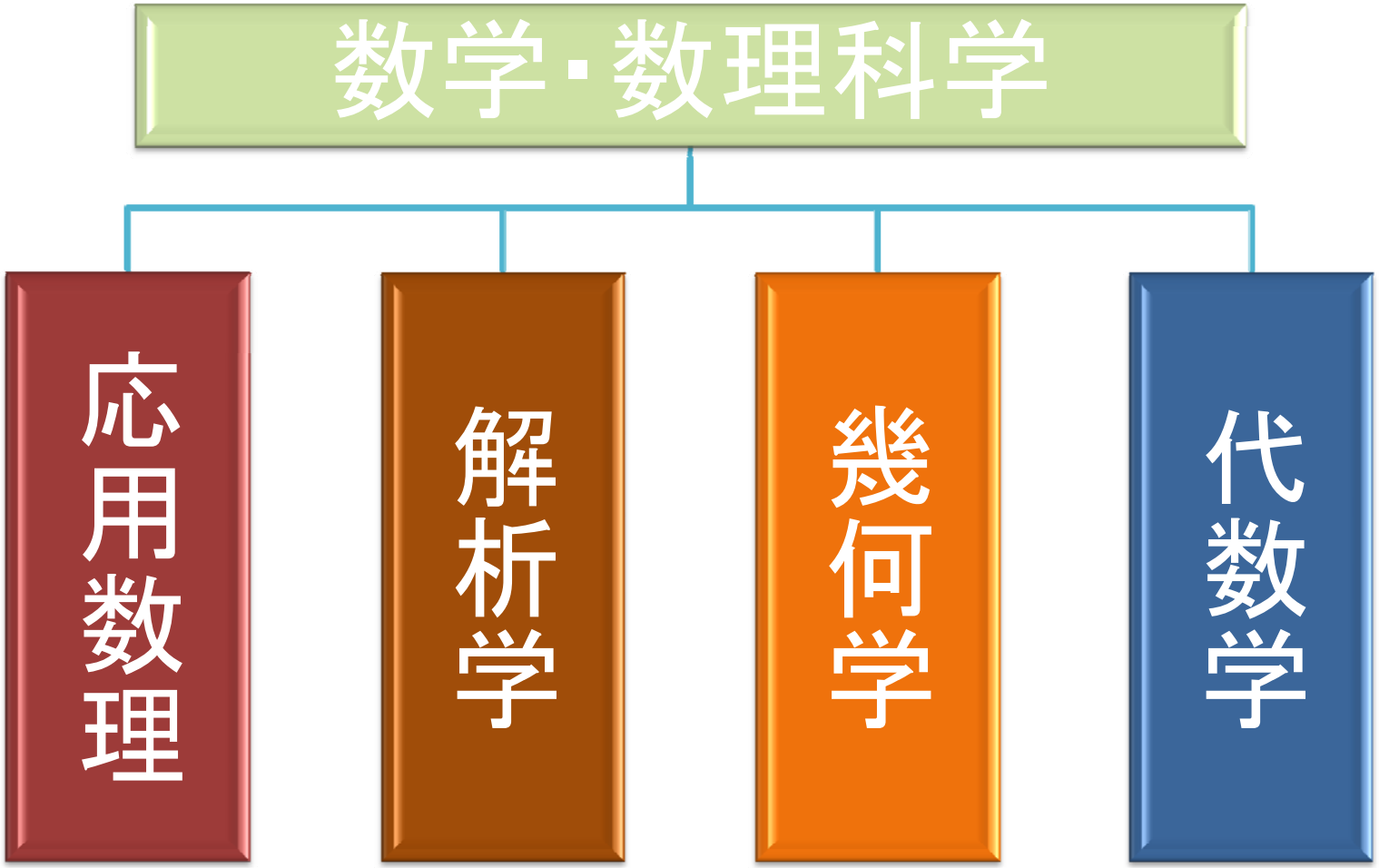
代数学の世界
―整数論とその応用―

第1回　初等整数論と有限の世界

東京大学大学院数理科学研究科
桂　利行

数学の分野図



1. 数について

自然数

$$\mathbb{N} = \{1, 2, 3, 4, \cdots\}$$

整数

$$\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$$

有理整数ということもある.

有理数

$$\mathbb{Q} = \{\cdots, 3, \frac{1}{2}, -\frac{5}{4}, \cdots\}$$

実数

$$\mathbb{R} = \{\cdots, 3, \frac{1}{2}, -\frac{5}{4}, \sqrt{2}, \pi, e, \cdots\}$$

複素数

$$\mathbb{C} = \{\cdots, 3, \frac{1}{2}, -\frac{5}{4}, \sqrt{2}, \pi, e, 2 + \sqrt{2}i, \cdots\}$$

$$i = \sqrt{-1}$$

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

これらの集合には

和　＋

積　×　・

の演算が与えられている。

代数系

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ の演算は次を満たす.

定義　集合 K に和 $+$, 積 $\cdot$ が定義されていて次をみたす時, K を**体**という.
$a, b, c \in K$ とする.

(I) (和 $+$ に関して)
- (i) (結合法則) $(a+b)+c = a+(b+c)$
- (ii) (零元の存在) 任意の $a \in K$ に対し, $0+a = a+0 = a$ となる元 0 が存在する.
- (iii) (和に関する逆元の存在) $a \in K$ に対し $a+a' = a'+a = 0$ となる元 $a' \in K$ が存在する.
- (iv) (可換性) $a+b = b+a$

(II) (積 $\cdot$ に関して)
- (i) (結合法則) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- (ii) (単位元の存在) 任意の $a \in K$ に対し $1 \cdot a = a \cdot 1 = a$ となる元 1 が存在する.
- (iii) (積に関する逆元の存在) $b \in K$, $b \neq 0$ に対し $b \cdot b' = b' \cdot b = 1$ となる元 $b' \in K$ が存在する.
- (iv) (可換性) $a \cdot b = b \cdot a$

(III) (分配法則)
- (i) $(a+b) \cdot c = a \cdot c + b \cdot c$
- (ii) $a \cdot (b+c) = a \cdot b + a \cdot c$

積を表す記号 $\times$ や $\cdot$ はしばしば省略され, $a, b \in K$ に対し, $a \times b$ や $a \cdot b$ をしばしば ab と書く.

- $\mathbb{Z}$ の演算は性質 (II)(iii) 以外を満たす.

定義　集合 R に和 $+$,積 $\cdot$ が定義されていて, 性質 (II)(iii) 以外の上記性質を満たす時, R を**可換環**という.

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ は無限に多くの元を含んでいる。

有限個元しか含まない体は存在するか

有限体

É. Galois　(1811-1832)

Sur la théorie des nombres.

(数の理論について.)

現 代

暗号理論, 符号理論への応用

‡　岩波数学事典第3版　日本数学会

著作権処理の都合で、

この場所に挿入されていた図版

“Galois論文”を

省略させていただきます。

※　ガロア全集より転載

2. 整数　$\mathbb{Z}$

素数

1と自分以外では割り切れない自然数

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \cdots$$

定理　素数は無限個存在する.

証明

背理法で示す.
素数が有限個しかないとする.
そのすべてを $p_1, p_2, \cdots, p_m$ とする.
$n = p_1 p_2 \cdots p_m + 1$　とおく.
n はある素数で割り切れるはず
$p_1, \cdots, p_m$ で割り切れない

矛盾

現在知られている最大の素数

$2^{32582657} - 1$　　(2006年9月)

桁数　　約 9808358 桁

$2^n - 1$ の形の素数　　メルセンヌ素数

現在　素数になる n が 44個知られている.

未解決問題

(1) **双子素数**は無限個存在するか。

偶数をはさんで両側が素数になるもの

3と5, 5と7, 11と13, 17と19, $\cdots$

現在知られている最大の双子素数

$$2003663613 \cdot 2^{195000} - 1$$

$$2003663613 \cdot 2^{195000} + 1$$

58711 桁　（2006年11月）

(2) ゴールドバッハ予想

４以上の偶数は2つの素数の和にかける。

$$
\begin{aligned}
4 &= 2+2 \\
6 &= 3+3 \\
8 &= 3+5 \\
10 &= 5+5 \\
12 &= 5+7 \\
&\vdots
\end{aligned}
$$

a, b : 整数

ある整数 q が存在して

$$b = aq$$

とかけるとき

- a は b を割り切る
- a は b の約数
- b は a の倍数

などという.

このとき $a \mid b$ とかく.

整数の基本的性質

(1)（剰余定理）

$$a, b \in \mathbb{Z},\ a \neq 0,\ b \neq 0$$

$$b = qa + r \qquad 0 \leq r < |a|$$

となるような整数q, r がただ1組存在する.

(2) 自然数は一意的に素因数分解される。

n : 自然数

有限個の素数 $p_1, \cdots, p_k \quad (i \neq j \text{ なら} p_i \neq p_j)$

自然数 $e_1, \cdots, e_k$

が存在して

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

と 積の順序を除いて一意的に表示される.

$a, b \in \mathbb{Z},\ a \neq 0,\ b \neq 0$

aとbの共通の約数　　公約数

aとbの公約数のうち最大のもの　　最大公約数
$\gcd(a, b)$

aとbの最大公約数が1になるとき，
aとbは互いに素であるという．

3. ユークリッドの互除法

補題

a, b を0でない2つの整数

$$a = qb + r \quad (q, r : \text{整数})$$

であるとする．このとき，$\gcd(a, b) = \gcd(b, r)$

0でない整数 a, b の最大公約数の求め方

順次 剰余定理を用いる.

$$
\begin{aligned}
a &= m_1 b + r_1 \ , \ 0 \leq r_1 \leq |b| - 1 \\
b &= m_2 r_1 + r_2 \ , \ 0 \leq r_2 \leq r_1 - 1 \\
r_1 &= m_3 r_2 + r_3 \ , \ 0 \leq r_3 \leq r_2 - 1 \\
r_2 &= m_4 r_3 + r_4 \ , \ 0 \leq r_4 \leq r_3 - 1 \\
&\vdots
\end{aligned}
$$

このとき, $r_1 > r_2 > \cdots \geq 0$ だから

自然数 n が存在して, $r_n \neq 0, \ r_{n+1} = 0$ となる.

このとき, $r_{n-1} = m_{n+1} \cdot r_n$

r_n が a, b の最大公約数

例

$$
\begin{aligned}
54 &= 2 \times 20 + 14 \\
20 &= 1 \times 14 + 6 \\
14 &= 2 \times 6 + 2 \\
6 &= 3 \times 2
\end{aligned}
$$

54 と 20 の最大公約数は 2

変形

$r_1 = a - m_1 b$

$p_1 = 1,\ q_1 = -m_1$ とおいて, $r_1 = p_1 a + q_1 b$

$r_2 = b - mr_1 = b - m_2(p_1 a + q_1 b) = -m_2 p_1 a + (1 - m_2 q_1) b$

$p_2 = -m_2 p_1,\ q_2 = 1 - m_2 q_1$ とおいて, $r_2 = p_2 a + q_2 b$

r_1, r_2 を3番目の式に代入すれば，同様に

$r_3 = p_3 a + q_3 b$ p_3, q_3 : 整数

以下，帰納的に

$r_i = p_i a + q_i b$ p_i, q_i : 整数

$i = n$ の時を考えれば, r_n は a, b の最大公約数だから

$\gcd(a, b) = r_n = p_n a + q_n b$ p_n, q_n : 整数

定理

a, b を0でない整数
a, b の最大公約数 d

このとき，整数 α, β で

$$\alpha a + \beta b = d$$

となるものが存在する.

系

a, b を互いに素な整数

このとき，整数 α, β で

$$\alpha a + \beta b = 1$$

となるものが存在する.

例

$a = 5,\ b = 7$

$x = 3,\ y = -2$ とすれば

$$3 \times 5 + (-2) \times 7 = 1$$

となる.

4. 合同

a, b, m　整数

$b - a$ が m で割り切れる $\Leftrightarrow$ $a \equiv b \pmod{m}$

合同式

性質

$a, b, c \in \mathbb{Z}$

(i) $a \equiv a \pmod{m}$

(ii) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$

(iii) $a \equiv b \pmod{m}$ かつ $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

整数mを1つ固定する.

$a \in \mathbb{Z}$に対し

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}$$

a の定める法mに関する **合同類** という.

a を $\overline{a}$ の代表元という.

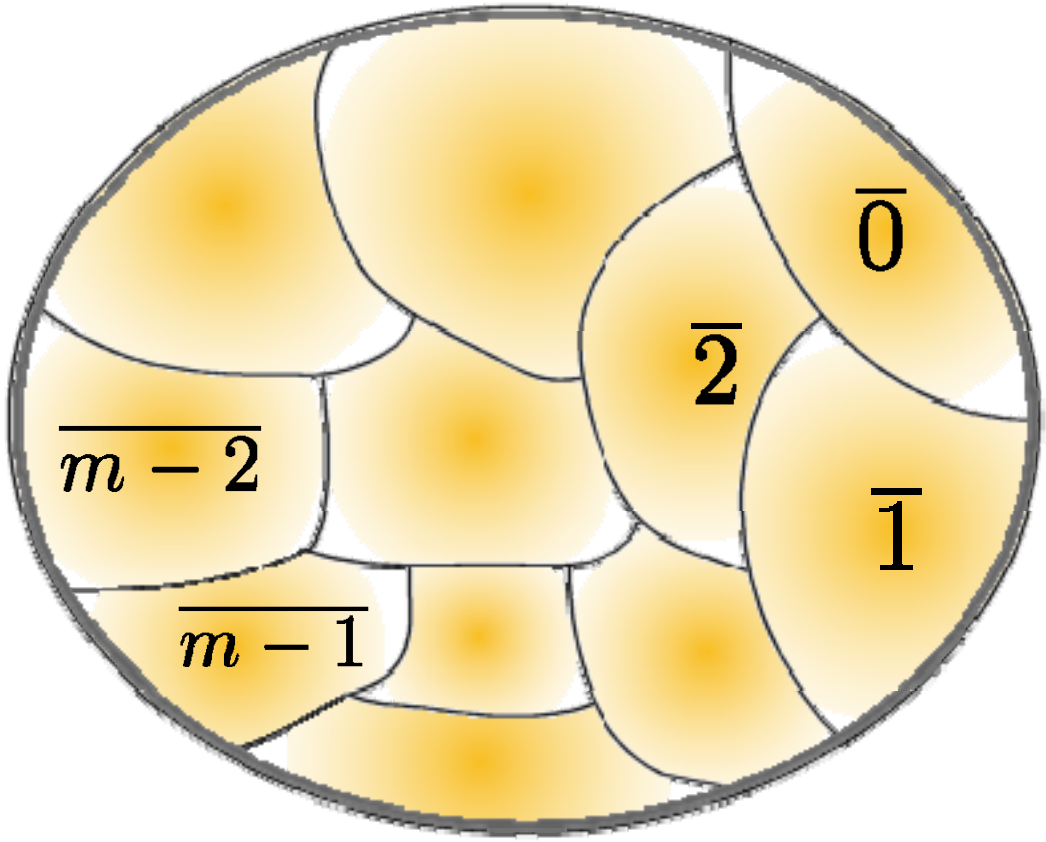
注意. $a \equiv b \pmod{m}$ なら $\overline{a} = \overline{b}$

法mに関する合同類全体の集合を

$$\mathbb{Z}/m\mathbb{Z}$$

とかく.

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{m-2}, \overline{m-1}\}$$



類の集合が $\mathbb{Z}/m\mathbb{Z}$

$\mathbb{Z}/m\mathbb{Z}$ には和と積の演算が自然にはいる.

補題 $a_1 \equiv a_2 \pmod{m},\ b_1 \equiv b_2 \pmod{m}$ ならば

$$a_1 \pm b_1 \equiv a_2 \pm b_2 \pmod{m}$$

$$a_1 b_1 \equiv a_2 b_2 \pmod{m}$$

- この補題は 類の代表をとりかえて演算を行っても結果として入る類はかわらないことを保証している.

$\mathbb{Z}/m\mathbb{Z}$ の和と積

$\overline{a}, \overline{b} \in \mathbb{Z}/m\mathbb{Z}$ に対し

和: $\overline{a} + \overline{b} = \overline{a+b}$

積: $\overline{a} \cdot \overline{b} = \overline{ab}$

と定義する.

零元 $\overline{0}$

$$\overline{a} + \overline{0} = \overline{0} + \overline{a} = \overline{a}$$

単位元 $\overline{1}$

$$\overline{a} \cdot \overline{1} = \overline{1} \cdot \overline{a} = \overline{a}$$

例

$$\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$$

たとえば $\overline{1} + \overline{2} = \overline{3},\ \overline{2} + \overline{3} = \overline{5} = \overline{1}$

$$\overline{2} \cdot \overline{2} = \overline{4} = \overline{0},\ \overline{2} \cdot \overline{3} = \overline{6} = \overline{2}$$

- $\mathbb{Z}/m\mathbb{Z}$ は可換環

  体になるとは限らない

例

$\mathbb{Z}/4\mathbb{Z}$ は体ではない.

$\overline{2} \cdot \overline{2} = \overline{0}$

$\overline{2}$ に逆元 $\overline{x}$ があるとすると

$\overline{2} \cdot \overline{x} = \overline{1}$ である.

$$\begin{array}{ccc} \overline{2} \cdot \overline{2} \cdot \overline{x} & = & \overline{0} \cdot \overline{x} \\ \| & & \| \\ \overline{2} = \overline{2} \cdot \overline{1} & & \overline{0} \end{array}$$

矛盾

$\mathbb{Z}/m\mathbb{Z}$の構造を理解するための補題

補題

$a, b, c, m \in \mathbb{Z}$
mとcは互いに素であるとする.

このとき

$$ac \equiv bc \pmod{m} \Rightarrow a \equiv b \pmod{m}$$

証明

mとcの最大公約数は1だから,
整数x, yで$cx + my = 1$となるものが存在.

$$a = acx + amy$$

$$b = bcx + bmy$$

故に,

$$a - b = (ac - bc)x + (ay - by)m$$

仮定から右辺はmで割り切れる.
故に$a - b$もmで割り切れる.

5. 有限体

$\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$

和　$\overline{0}+\overline{0}=\overline{0}$, $\overline{0}+\overline{1}=\overline{1}$

$\overline{1}+\overline{0}=\overline{1}$, $\overline{1}+\overline{1}=\overline{0}$

積　$\overline{0}\cdot\overline{0}=\overline{0}$, $\overline{0}\cdot\overline{1}=\overline{0}$

$\overline{1}\cdot\overline{0}=\overline{0}$, $\overline{1}\cdot\overline{1}=\overline{1}$

体になる.

p を素数とする.

$$\mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{p-1}\}$$

和　$\overline{a}+\overline{b}=\overline{a+b}$

積　$\overline{a}\cdot\overline{b}=\overline{ab}$

定理　p を素数とすれば，$\mathbb{Z}/p\mathbb{Z}$ は体になる．

証明

$\overline{0}$　零元

$\overline{1}$　単位元

$\overline{0}$ でない任意の元 $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$ に逆元があることを示せばよい．

p が素数で，$\overline{a} \neq \overline{0}$ より，a と p は互いに素．

整数 x, y が存在して

$$1 = xa + yp$$ となる．

法 p で考えれば

$$\overline{1} = \overline{xa + yp} = \overline{x}\,\overline{a} + \overline{y}\,\overline{p} = \overline{x}\,\overline{a} + \overline{y}\,\overline{0} = \overline{x}\,\overline{a}$$

$\overline{x}$ は $\overline{a}$ の逆元！

定義　p　素数

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$　とおく.

$\mathbb{F}_p$ は p 個の元からなる有限体

注意1　$\mathbb{Z}/m\mathbb{Z}$ が体 ⇔　m が素数

注意2　nを自然数, pを素数とするとき,
p^n 個の元を持つ有限体 $\mathbb{F}_{p^n}$が
ただ1つ存在することが知られている.
また,　有限体は$\mathbb{F}_{p^n}$　(n　自然数, p　素数)
しか存在しない.