

科学・技術の世界 – Fermat の大定理を巡って –

第四回 平成17年5月10日(火)

†:このマークが付してある著作物は、第三者が有する著作物ですので、同著作物の再使用、同著作物の二次的著作物の創作等については、著作権者より直接使用許諾を得る必要があります。

先々週の補足(1/2)

前回の授業で口頭でのみ示したことを以下に列挙する.

- Gauss の学位論文の主張は「 n 次方程式は複素数では必ず解ける」こと.
- しかるに Abel が主張したことは「一般の 5 次以上の方程式を解く解の公式は存在しない」.
- Abel, Gauss とともに現在の知見で間違ったことは言っていないことがわかっている.

先々週の補足(2/2)

- Fermat の小定理を利用した素数判定では素数でないことがわかっていても素因数はわからない. 現在に至るまで素因数そのものを見付けることは非常に難しく,これが暗号の強度を保証するものとなっている.
- また,上記の素数判定法では「素数である」ことは判定できない. 例として 561 は上記の判定法では素数でないことは判定できないが, $561 = 3 \times 11 \times 17$ である. このような数をカーマイケル数という.
- 尚,与えられた数の素因数を求める問題は P であることが証明されている (2003).

Descartes の考え (1/2)

Fermat と同時代の数学者に Descartes がいる.

Fermat と Descartes は 1637–38 にかけて Descartes の幾何光学について論争を行い, これが Fermat の名をヨーロッパで有名にした. ここでは Descartes の「幾何学」から彼の基本的な考え方を抜粋しておく.

- いちばん単純で, いちばん認識しやすいものを一種の公理とする.
- どんなに難しい, 遠いものでも, 単純なやさしい推論を重ねていけば必ずたどりつくことができる.
- 証明できないものは一切信用しない.



足立恒雄 (1994, 2006), フェルマーの大定理—整数論の源流, 日本評論社/ちくま学芸文庫, より引用

Descartes の考え (2/2)

しかしながら, Descartes の数学という学問に対する見方は次のようなものであった.

- 真理を摂取し, まちがった論拠では少しも満足しない習慣をそうしたものが精神に付けてくれること以外は, 何の効用も期待していない.

こうした考えを持つのは Descartes だけでなく, 後に紹介する Pascal も同様であった.



足立恒雄 (1994, 2006), フェルマーの大定理—整数論の源流, 日本評論社/ちくま学芸文庫, より引用

補遺

Decartes の考え方は現在にも受け継がれているが、公理の一部に変化が見られる。

- 単純でなくても, (たとえ直感に反しても) その他の現象が一番たやすく説明出来るものを一種の公理とする.
- どんなに難しい, 遠いものでも, 単純なやさしい推論を重ねていけば必ずたどりつくことができる.
- 証明できないものは一切信用しない.

同値関係

集合 G の元の間で以下の三つの条件を満たすものを同値条件という.

- $a \equiv a$ (反射律)
- $a \equiv b$ であれば $b \equiv a$ (対称律)
- $a \equiv b, b \equiv c$ であれば $a \equiv c$ (推移律)

同値関係の例 (1/2)

$G = \mathbb{Z}$ とし, 自然数 n を固定する.

$$a \equiv b \Leftrightarrow a - b \text{ は } n \text{ で割り切れる.}$$

検証 $n = 5$ とする.

- $a - a = 0$ は常に 5 で割り切れる.
- $a - b$ が 5 で割り切れれば, $b - a$ も 5 で割り切れる.
- $a - b, b - c$ が 5 で割り切れれば,
 $a - b - (b - c) = a + c$ も 5 で割り切れる.

同値関係の例 (2/2)

$G = \mathbb{Z} + i\mathbb{Z}$ (Gauss 整数) とし, Gauss 整数 $a + bi$ を固定する.

$$x \equiv y \Leftrightarrow x - y \text{ は } a + bi \text{ の倍数.}$$

は同値関係となる.

$G = x$ を変数とする $\mathbb{C}$ 係数の多項式の集合 とし, 多項式 $h(x)$ を固定する.

$$f(x) \equiv g(x) \Leftrightarrow f(x) - g(x) \text{ は } h(x) \text{ で割り切れる.}$$

も同値関係となる.

同値類と代表元(1/3)

集合 G に同値関係 $\equiv$ が定義されているとき, 同値な元からなる部分集合を同値類という.

例 1 $G = \mathbb{Z}$, $a \equiv b \Leftrightarrow a - b$ が 3 で割り切れる, と定義したとき,

- 0 と同値なものは $3, 6, 9, \dots, 3n$
- 1 と同値なものは $4, 7, 10, \dots, 3n + 1$
- 2 と同値なものは $5, 8, 11, \dots, 3n + 2$

全ての整数は上の三つの部分集合のどれかに含まれる. よって同値類は三つある.

例 2 $G = \mathbb{Z}$ とし, 今度は $a \equiv b \Leftrightarrow a - b$ が 8 で割り切れる, と定義すると同値類の数は 8 個ある.

同値類と代表元(2/3)

例 3 $G = \mathbb{R}[x]$ (実数係数の多項式の集合) とし,
 $f(x) \equiv g(x) \Leftrightarrow$
 $f(x) - g(x)$ が $x^2 + 1$ で割り切れる, と定義する.

- $f(x)$ を $x^2 + 1$ で割った余りは必ず一次式なので, それを $ax + b$ とすると, $f(x) \equiv ax + b$.
- $ax + b \equiv cx + d$ であるのは $a = c, b = d$ であるとき, またそのときに限る.
- 以上からこの場合の同値類の個数は無限個あるが, それらは一次式 $ax + b$ と一対一対応があることがわかる.

同値類と代表元(3/3)

各同値類の中から, 一つずつ元を選んだものを代表元の集合と呼ぶ. 先の例で見れば,

- $G = \mathbb{Z}$, $a \equiv b \Leftrightarrow a - b$ が 3 で割り切れる, とした場合の代表元の集合として $\{0, 1, 2\}$ が取れる.
- 代表元のとりかたは一通りではない. 上の場合 $\{-1, 0, 1\}$ などもありうる.
- $G = \mathbb{Z}$, $a \equiv b \Leftrightarrow a - b$ が 8 で割り切れる, とした場合の代表元の集合として $\{0, 1, 2, 3, 4, 5, 6, 7\}$ が取れる.

同値類の演算 (1/4)

整数の集合 $G = \mathbb{Z}$ に対し,
 $a \equiv b \Leftrightarrow a - b$ が n で割り切れる, と同値関係を定義する. また a が属する同値類を $\{a\}$ と書くことにする. $a, b \in G$ に対して, $\{a\}$ の代表元を x , $\{b\}$ の代表元を y とすると, x, y の選び方によらず

$$x + y \in \{a + b\}, \quad xy \in \{ab\}$$

が成立する. これから同値類 $\{a\}, \{b\}$ の和, 積を

$$\{a\} + \{b\} := \{a + b\}, \quad \{a\} \cdot \{b\} := \{ab\}$$

と定義する.

同値類の演算 (2/4)

$n = 5$ のとき実際に計算を試みる.

$$\{12\} + \{3\} = \{12 + 3\} = \{15\} = \{0\}$$

$$= \{\textcolor{red}{2} + 3\} = \{5\} = \{0\}$$

$$\{2\} - \{8\} = \{2 - 8\} = \{-6\} = \{4\}$$

$$= \{2 - \textcolor{red}{3}\} = \{-1\} = \{4\}$$

$$\{13\} \cdot \{11\} = \{3 \cdot 1\} = \{3\}$$

$$\{3\}^4 = \{3^4\} = \{81\} = \{1\}$$

$$\{3\}^{17} = \{3\}^{16} \cdot \{3\} = \{3^4\}^4 \cdot \{3\} = \{3\}$$

同値類の演算 (3/4)

n の値によっては同値類同士の割り算が定義できる. まず例を以下にあげる. まず $n = 5$ のとき,

$$\{2\} \div \{3\} = \{12\} \div \{3\} = \{12 \div 3\} = \{4\}$$

$$\{1\} \div \{3\} = \{6\} \div \{3\} = \{6 \div 3\} = \{2\}$$

$n = 7$ のとき,

$$\{3\} \div \{4\} = \{24\} \div \{4\} = \{24 \div 4\} = \{6\}$$

$$\{1\} \div \{5\} = \{15\} \div \{5\} = \{15 \div 5\} = \{3\}$$

$$= \{50\} \div \{5\} = \{50 \div 5\} = \{10\} = \{3\}$$

同値類の演算 (4/4)

前項での計算規則をまとめると以下のようになる.

- $\{a\} = \{a + kn\}$ であることを利用し, 割られる数に n の倍数を加えて, 割り切れるようにして, 割り算を実行する.

これで割り算が出来るか? という以下の疑問が沸く.

- 割られる数に n の倍数を加えることで, **必ず** 割り切れるようにできるのか?
- 加える n の倍数の値にかかわらず, 計算結果はいつも同じになるのか?

結論としては n が素数であれば, 上記二項は成立する.

合同式

これまでと同様に $G = \mathbb{Z}$ に対し,
 $a \equiv b \Leftrightarrow a - b$ が n で割り切れる, と定義する. このとき二つの整数 c, d が同じ同値類を定めることを

$$c \equiv d \pmod{n}$$

と書く. 前項までの演算規則をこの記号を使って書き直すと以下のようなになる.

$$\begin{aligned} a \equiv b, c \equiv d & \pmod{n} \\ \Rightarrow a + b \equiv c + d, \quad ab \equiv cd & \pmod{n} \end{aligned}$$

これから同値関係 $\equiv$ は等式 $=$ と似た性質を持つことがわかる.

Fermat の小定理 (再)(1/4)

これまでに見てきた同値関係を使って Fermat の小定理をもう一度考えてみる. まず定理自身を書き直す.

定理 **1** p を素数とする. このとき, 任意の整数 m に対して

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

が成立する.

Fermat の小定理 (再)(2/4)

証明の前に具体的な計算をする. $p = 7$ とし $m = 5$ とする.

$$5 \cdot 1 \equiv 5 \pmod{7}$$

$$5 \cdot 2 \equiv 10 \equiv 3 \pmod{7}$$

$$5 \cdot 3 \equiv 1 \pmod{7}$$

$$5 \cdot 4 \equiv 6 \pmod{7}$$

$$5 \cdot 5 \equiv 4 \pmod{7}$$

$$5 \cdot 6 \equiv 2 \pmod{7}$$

これらの式を辺々掛け併せ, $6!$ で割ると,

$$5^{7-1} \cdot 6! \equiv 6! \pmod{7} \Rightarrow 5^{7-1} \equiv 1 \pmod{7}.$$

Fermat の小定理 (再)(3/4)

m と $i = 1, \dots, p-1$ の積を考え,

$$m \cdot i \equiv m_i \pmod{p}$$

とおく. ここで m_i は $1, \dots, p-1$ のいずれかの数であることに注意する. $m_i \equiv m_j$ とすると,

$$m_i \equiv m_j \Rightarrow m \cdot i \equiv m \cdot j \Rightarrow i \equiv j$$

となるので, 集合として $\{m_i\}$ は $\{1, \dots, p-1\}$ に等しい.

Fermat の小定理 (再)(4/4)

これから, m_i の積を取ると,

$$(m \cdot 1) \cdots (m \cdot (p-1)) \equiv m_1 \cdots m_{p-1} \pmod{p}$$

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

上の両辺を $(p-1)!$ で割ることで, 求める式

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

を得る.

Euler の定理

Fermat の小定理は p が素数でない場合には以下のように拡張できる.

定理 2 整数 n に対し, 函数 ϕ を

$\phi(n) := \{1, \dots, n-1\}$ で n と互いに素な数の個数

とする. このとき, 任意の整数 m に対し,

$$m^{\phi(n)-1} \equiv 1 \pmod{n}$$

が成立する.