東海大学紀要情報通信学部
Vol.11,No.1,2018,pp.31-37

トピックス

大学初年次における数学教材の提案（その 19）
～中国式剰余定理～

貴田 研司[*1]

A Suggestion on Mathematical Materials for Freshman Education Vol.19
~ Chinese Remainder Theorem ~

by

Kenshi KIDA[*1]

(received on May 30, 2018 & accepted on Jul.27, 2018)

あらまし

整数論においては，計算に不可欠な方法の一つにユークリッドの互除法がある．この方法に関連するものとして，連立一次合同方程式を解く手段としての中国式剰余定理について述べる。

Abstract

As an essential method of caluculations in number theory, we present the Euclidean algorithm. Furthermore, we present the Chinese remainder theorem as a means to solve systems of linear congruence equations .

キーワード: 初等整数論, ユークリッドの互除法, 中国式剰余定理, 連立一次合同方程式

Keywords: *Elementary Number Theory , Euclidean Algorithm, Chinese Remainder Theorem , System of Linear Congruence Equations*

1. はじめに

まず，整数論において重要である，合同の概念と合同式について述べる．

定義（合同式）

2 つの整数a,bについて，$a-b$がmの倍数となるとき，aとbはmを法として合同であるといい

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

と表す．

定理 1.1

$a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$ ならば

$$a+c \equiv b+d \pmod{m}$$

$$a-c \equiv b-d \pmod{m}$$

$$a \times c \equiv b \times d \pmod{m}$$

が成り立つ．

*1 高輪教養教育センター 准教授
Liberal Arts Education Center, Takanawa Campus,
Associate Professor

よって，類の代表元をどのように選んだとしても，加減乗の結果として決まる類は一意的に決定されることがわかる．したがって，m 個の類からなる商集合$\mathbb{Z}/m\mathbb{Z}$ に，加減乗の二項演算を定義することができる．以下のようになる．

定義

$$a \pmod m + b \pmod m = (a+b) \pmod m$$

$$a \pmod m - b \pmod m = (a-b) \pmod m$$

$$a \pmod m \times b \pmod m = (a \times b) \pmod m$$

また，整数a, b に対して

$$ax \equiv b \pmod m$$

のような形の方程式を，1 次合同方程式という．

本論文では，整数論において，計算に不可欠な方法の一つであるユークリッドの互除法と，この方法と関連の深い中国式剰余定理について解説する[1)2)3)4)5)]．

2. ユークリッドの互除法

この章では，ユークリッドの互除法とその適用された例について述べる．

定理 2.1

$a > b > 0$ を整数，a をbで割った商をq，余りをr，すなわち

$$a = bq + r$$

とする．このとき

$$(a, b) = (b, r)\big(= (a - bq, b)\big)$$

が成り立つ．

この定理を繰り返して用いることにより，a と b の最大公約数(a, b)を求めることができる．

これをユークリッドの互除法という．

例題 2.1

255 と183 の最大公約数$(255, 183)$ を，ユークリッドの互除法を用いて求めよ．

（解答）

$$255 = 1 \times 183 + 72 \cdots\cdots ①$$

$$183 = 2 \times 72 + 39 \cdots\cdots ②$$

$$72 = 1 \times 39 + 33 \cdots\cdots ③$$

$$39 = 1 \times 33 + 6 \cdots\cdots ④$$

$$33 = 5 \times 6 + 3 \cdots\cdots ⑤$$

$$6 = 2 \times 3$$

であるから

$$(255, 183) = 3$$

が得られる．

（解答終）

定理 2.2

a, b を整数とするとき，a と b の最大公約数 $d = (a, b)$ は，適当な整数 x, y によって

$$d = ax + by$$

と表すことができる．

例題 2.2

例題 2.1 において，$(255, 183) = 3$ であることがわかった．適当な整数 x, y によって

$$3 = 255x + 183y$$

の形に表せ．

（解答）

⑤より

$$3 = 33 - 5 \times 6 \cdots\cdots ㋐$$

④より，$6 = 39 - 1 \times 33$ なので

$$㋐ = 33 - 5 \times (39 - 1 \times 33)$$

$$= (-5) \times 39 + 6 \times 33 \cdots\cdots ㋑$$

③より，$33 = 72 - 1 \times 39$ なので

$$㋑ = (-5) \times 39 + 6 \times (72 - 1 \times 39)$$

$$= 6 \times 72 + (-11) \times 39 \cdots\cdots ㋒$$

②より，$39 = 183 - 2 \times 72$ なので

$$㋒ = 6 \times 72 + (-11) \times (183 - 2 \times 72)$$

$$= (-11) \times 183 + 28 \times 72 \cdots\cdots ㋓$$

①より，$72 = 255 - 1 \times 183$ なので

$$㋓ = (-11) \times 183 + 28 \times (255 - 1 \times 183)$$

$$= 28 \times 255 + (-39) \times 183$$

したがって

$$3 = 255 \times 28 + 183 \times (-39)$$

と表すことができる．

（解答終）

3. 中国式剰余定理

第 2 章で紹介したユークリッドの互除法から得られる結果として次のような定理がある．

定理 3.1

1 次合同式$ax \equiv b \pmod{m}$ は，b が$(a,m) = d$ の倍数であるときのみ解をもち，その解の個数はm を法としてd 個である．特に、$(a,m) = 1$ のとき，この 1 次合同式はm を法としてただ一つの解をもつ．

例

$(a,m) = 1$ のとき，$ax \equiv 1 \pmod{m}$ の解は一意的に定まる．これを類の乗法で言えば，$a \pmod{m}$ の逆元にあたる，すなわち，

$$a \pmod{m} \times x \pmod{m} = 1 \pmod{m}$$

が成り立つ．

定理 3.2（中国式剰余定理）

$m_1, m_2, \cdots, m_n$ を，どの 2 つをとっても互いに素であるような整数としたとき，連立 1 次合同方程式

$$x \equiv b_1 \pmod{m_1} \qquad (1)$$

$$x \equiv b_2 \pmod{m_2} \qquad (2)$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$x \equiv b_n \pmod{m_n} \qquad (n)$$

は，積$M = m_1 m_2 \cdots m_n$ を法として，ただ一つの解をもつ．

（証明）

まず，

$$M_i = \frac{M}{m_i} \qquad (i = 1,2,\cdots,n)$$

とすると，仮定から$(m_i,\ M_i) = 1 \quad (i = 1,2,\cdots,n)$ であることがわかる．したがって、定理3.1から

$$M_i f_i \equiv 1 \pmod{m_i} \qquad (i = 1,2,\cdots,n)$$

を満たす整数f_i $(i=1,2,\cdots,n)$ が求められる．

$$t_i = M_i f_i \quad (i=1,2,\cdots,n)$$

とすると，M_i はm_j $(j \neq i)$ の倍数であるから

$$t_i \equiv 1 \pmod{m_i}, \qquad t_i \equiv 0 \pmod{m_j} \quad (j \neq i)$$

となっていることがわかる．これより

$$b_k t_k \equiv b_k \pmod{m_k}, \qquad b_l t_l \equiv 0 \pmod{m_k} \quad (l \neq k)$$

なので

$$t_1 b_1 + t_2 b_2 + \cdots + t_n b_n \equiv b_k \pmod{m_k} \quad (k=1,2,\cdots,n)$$

であるから

$$x = t_1 b_1 + t_2 b_2 + \cdots + t_n b_n$$

が1つの解である．

もしも

$$y \equiv b_1 \pmod{m_1} \qquad (1)'$$

$$y \equiv b_2 \pmod{m_2} \qquad (2)'$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$y \equiv b_n \pmod{m_n} \qquad (n)'$$

であれば，対応する式を引いて

$$x - y \equiv 0 \pmod{m_1} \qquad (1)''$$

$$x - y \equiv 0 \pmod{m_2} \qquad (2)''$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$x - y \equiv 0 \pmod{m_n} \qquad (n)''$$

を得るが，これは$x-y$が，どの2つをとっても互いに素な，$m_1, m_2, \cdots, m_n$の倍数であることを意味している．

したがって，$x-y$はこれらの最小公倍数$M = m_1 m_2 \cdots m_n$で割り切れるので，$x - y \equiv 0 \pmod{M}$ すなわち $x \equiv y \pmod{M}$ なので，2つの解xとyは，Mを法として一致する．

（証明終）

例題3.1

3で割れば2が余り，7で割れば5が余り，8で割れば4余る整数を求めよ．

（解答）

連立1次合同方程式で表すと

$$x \equiv 2 \pmod 3 \qquad (1)$$

$$x \equiv 5 \pmod 7 \qquad (2)$$

$$x \equiv 4 \pmod 8 \qquad (3)$$

となる．定理3.2の証明での記号をそのまま使うことにすると

$$M = 3 \times 7 \times 8 = 168,$$

$$M_1 = 7 \times 8 = 56,$$

$$M_2 = 3 \times 8 = 24,$$

$$M_3 = 3 \times 7 = 21$$

である．すると$(3,56) = 1,\ (7,24) = 1,\ (8,21) = 1$ なので，定理3.1から

$$56f_1 \equiv 1 \pmod 3,\ 24f_2 \equiv 1 \pmod 7,\ 21f_3 \equiv 1 \pmod 8$$

を満たすような整数$f_1,\ f_2,\ f_3$が求められることがわかる．求めてみると

$$f_1 \equiv -1 \pmod 3,\quad f_2 \equiv -2 \pmod 7,\quad f_3 \equiv 5 \pmod 8$$

である．そこで

$$t_1 = M_1 f_1 = 56 \times (-1) = -56,\ t_2 = M_2 f_2 = 24 \times (-2) = -48,\ t_3 = M_3 f_3 = 21 \times 5 = 105$$

とすると，解は

$$\begin{aligned} x &\equiv t_1 b_1 + t_2 b_2 + t_3 b_3 \\ &= (-56) \times 2 + (-48) \times 5 + 105 \times 4 \\ &= -112 - 240 + 420 \\ &= 68 \pmod{168} \end{aligned}$$

となる．

したがって，xは$68 + 168k \quad (k \in \mathbb{Z})$の形の整数である．

（解答終）

4. おわりに

中国式剰余定理は，一般の環論において以下のように拡張される[6]．

定理 4.1(Chinese remainder Theorem)

Rを可換環とし，$I_1, I_2, \cdots, I_n$はどの2つも互いに素であるイデアル$\left(I_k + I_l = R \quad (k \neq l)\right)$とする．このとき$R$の任意の$n$個の元$a_1, a_2, \cdots, a_n$に対して

$$x \equiv a_1 \pmod{I_1}$$

$$x \equiv a_2 \pmod{I_2}$$

$$\cdots\cdots\cdots\cdots\cdots$$

$$x \equiv a_n \pmod{I_n}$$

を満たす元$x \in R$が存在する.

定理 4.2

Rを可換環とし，$I_1, I_2, \cdots, I_n$はどの 2 つも互いに素であるイデアル$\left(I_k + I_l = R \quad (k \neq l)\right)$とする．このとき

$$R/(I_1 \cap I_2 \cap \cdots \cap I_n) \simeq R / I_1 \oplus R / I_2 \oplus \cdots\cdots \oplus R / I_n$$

となる.

参考文献

1) 草場公邦「ガロアと方程式」朝倉書店，1989
2) 高木貞治「初等整数論講義 第2版」共立出版，1971
3) 楫元「工科系のための初等整数論入門-公開鍵暗号をめざして-」培風館，2000
4) 野崎昭弘「離散系の数学」近代科学社，1980
5) 雪江明彦「整数論1　初等整数論からp進数へ」日本評論社，2013
6) 永尾汎「代数学」朝倉書店，1983