「代数学序論」講義ノート

那須弘和 *

2020 年度春学期 †

はじめに

本講義ノートは, 2020 年 5 月から 7 月にかけて東海大学理学部情報数理学科において行われた講義「代数学序論」の講義ノート[*1] である. 本講義では初等整数論の基礎について学ぶ. 初等整数論は代数学発祥の分野である. 近年情報科学における暗号や符号理論などの実用的な分野でも活用されている. 代数学序論では整数の割り算定理から出発し, 基本的な諸定理を積み重ねる. 整数論の論法に慣れるようにできる限り多くの具体例を挙げながら解説したい.

講義内容に関する理解を深める為にも, 講義のあと必ず演習問題を取り組んで欲しい.

目次

* 東海大学理学部情報数理学科, E-mail: nasu@tokai-u.jp

† 2020 年 9 月 24 日更新

*1 他の講義資料に関しては Web サイトを参照のこと：http://fuji.ss.u-tokai.ac.jp/nasu/2020/alg0.html

1　整数の除算定理, 約数と倍数

整数全体の集合を $\mathbb{Z}$, 自然数全体の集合を $\mathbb{N}$ で表す.

定義 1.1. a, b を零でない整数とする. ある整数 q に対し, $a = qb$ を満たすとき,

- a は b で**割り切れる**,
- a は b の**倍数**である, または
- b は a の**約数**である,

という. 記号では $b|a$ と表す.

例 1.2. 6 の約数は $-6, -3, -2, -1, 1, 2, 3, 6$ であり, 全部で 8 個存在する. 一方 6 の倍数は 0 と正の倍数が $6, 12, 18, \ldots$ と無限に続き, 負の倍数も $-6, -12, \ldots,$ と無限に存在する.

命題 1.3. 整数 $a_1, \ldots, a_n$ が整数 b の倍数ならば, 任意の整数 $x_1, \ldots, x_n$ に対し

$$a_1x_1 + \cdots + a_nx_n$$

は b の倍数である.

次が除法の定理 (割り算の定理) と呼ばれる.

命題 1.4. 整数 a と自然数 b に対し

$$a = qb + r \qquad \text{かつ} \qquad 0 \leq r < b$$

を満たす整数の組 (q, r) が唯一つ存在する.

q と r をそれぞれ a を b で割ったときの**商**と**余り**と呼ぶ.

例 1.5. 204 を 85 で割ると,

$$204 = 2 \times 85 + 34 \qquad \text{かつ} \qquad 0 < 34 < 85$$

から商は 2 となり, 余りは 34 となる.

1.1　最大公約数と最小公倍数

定義 1.6. 整数 a, b に対し, $a \neq 0$ または $b \neq 0$ のとき, それらの共通の約数のうちで最大のものを**最大公約数**といい, 記号 $\gcd(a, b)$(または記号 (a, b)) により表す.

例 1.7. 18 と 24 の最大公約数は 6 である. すなわち $\gcd(18, 24) = 6$ となる.

整数 a, b に対して, $(a, b) = (b, a)$ が成り立つ. 任意の $a > 0$ に対し, $(a, 0) = a$ となる.

命題 1.8. 整数 a, b に対し次が成り立つ:

(1) a, b の公倍数は, 最小公倍数の倍数である.
(2) a, b の公約数は, 最大公約数の約数である.

(3) 自然数 a, b に対し, a と b の最大公約数を d, 最小公倍数を m とすれば, $ab = dm$ が成り立つ.

定義 1.9. 整数 a, b の最大公約数が 1 に等しいとき, すなわち $(a, b) = 1$ のとき, a と b は**互いに素である**という.

1.2 ユークリッドの互除法

命題 1.10. 整数 a, q と自然数 b に対して,

$$(a, b) = (a - qb, b)$$

が成り立つ. とくに, a の b による割り算の余りを r とすれば

$$(a, b) = (b, r)$$

が成り立つ.

証明) $\mathbb{Z}$ の部分集合 X, Y を

$$X = \{a \text{ と } b \text{ の公約数 }\} \qquad Y = \{a - qb \text{ と } b \text{ の公約数 }\}$$

と定める. 命題 1.10 の証明には $X = Y$ を示せば十分である. 実際, 命題は X と Y の最大元が一致することを主張するものである.

まず $X \subset Y$ を示す. X の任意の元を x とすれば, $a = kx$ と $b = lx$ をともに満たす整数 k, l が存在する.

$$a - qb = kx - q(lx) = (k - ql)x$$

であるので, x は $a - qb$ と b の公約数であり, $x \in Y$, すなわち $X \subset Y$ がわかる.

次に $Y \subset X$ を示す. Y の任意の元を y とすれば, $a - qb = k'y$ と $b = l'y$ をともに満たす整数 k', l' が存在する. このとき

$$a = (a - qb) + qb = k'y + q(l'y) = (k' + ql')y$$

であるので y は a の約数である. したがって $y \in X$, すなわち $Y \subset X$ が示された. □

定理 1.11 (ユークリッドの互除法)**.** 自然数 a, b に対して, 次の操作を考える:

[1] a の b による割り算の余りを r_1 とする.
[2] b の r_1 による割り算の余りを r_2 とする.
[3] r_1 の r_2 による割り算の余りを r_3 とする.

以下同様にして $r_{i-1} \neq 0$ である限り,

[i] r_{i-2} の r_{i-1} による割り算の余りを r_i とする.

を繰り返す. このときある有限の i に対し, $r_i = 0$ となる i が存在する. $r_n \neq 0$ かつ $r_{n+1} = 0$ とすれば,

$$(a, b) = r_n$$

が成り立つ. すなわち r_n は a, b の最大公約数に等しい.

定理 1.11 において $a > b$ である必要はなく $a < b$ であっても良い. (その場合にはステップ [1] で商が 0, 余りが a になる.)

証明) 定理の操作のステップから,

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ r_2 &= q_4 r_3 + r_4 \\ &\vdots \\ r_{i-2} &= q_i r_{i-1} + r_i \end{aligned}$$

となる. 余り r_i については

$$b > r_1 > r_2 > \cdots > r_{i-1} > r_i > \cdots$$

を満たす. 全て非負の整数なので有限回のステップで必ず $r_i = 0$ となる. 例えば $r_{n-1} = q_{n+1} r_n$ ならば $r_{n+1} = 0$ であり, 命題 1.10 により,

$$(a, b) = (b, r_1) = \cdots = (r_{n-1}, r_n) = r_n$$

となる. □

ユークリッドの互除法アルゴリズムについては次の定理が知られている.

定理 1.12 (ラメの定理)**.** 自然数 a, b に対して, $a > b$ とし, b を 10 進数表示したときの桁数を s とする. このとき a, b に対しユークリッド互除法アルゴリズムを適用すると, 最大 $5s$ 回の割り算でアルゴリズムは終了する.

たとえば 10 進数表示で 3 桁の自然数にユークリッドの互除法を適用する場合, せいぜい 15 回も割り算を行えば最大公約数が求まる.

例 1.13. $a = 391$ と $b = 221$ の最大公約数をユークリッド互除法アルゴリズムにより求める.

$$\begin{aligned} 391 &= 221 \times 1 + 170 \\ 221 &= 170 \times 1 + 51 \\ 170 &= 51 \times 3 + 17 \\ 51 &= 17 \times 3 \end{aligned}$$

より, $\gcd(391, 221) = 17$ となる.

2 一次不定方程式

定義 2.1. 整数 a, b, c に対し x, y を未知数とする一次方程式

$$ax + by = c, \qquad ab \neq 0 \tag{2.1}$$

の整数解 x, y を求める問題で, この方程式を**一次不定方程式**または**ディオファントス方程式**と呼ぶ.

2.1　拡張されたユークリッドの互除法

整数 a と b に対し, a と b の最大公約数を d とする. ユークリッドの互除法アルゴリズムを用いれば, 一次不定方程式

$$ax + by = d \tag{2.2}$$

の一組の解 (x, y) を与えることが可能である. $a = 391$ と $b = 221$ に対し, a と b の最大公約数 $d = 17$ を求めた例 1.13 を用いて, 一次不定方程式 $391x + 221y = 17$ の一組の解を与える.

$$391 = 221 \times 1 + 170 \tag{2.3}$$
$$221 = 170 \times 1 + 51 \tag{2.4}$$
$$170 = 51 \times 3 + 17 \tag{2.5}$$
$$51 = 17 \times 3 \tag{2.6}$$

(2.5),(2.4),(2.3) の順番に式を用いると

$$\begin{aligned} 17 &= 170 - 51 \times 3 \\ &= 170 - (221 - 170 \times 1) \times 3 \\ &= 170 \times 4 - 221 \times 3 \\ &= (391 - 221 \times 1) \times 4 - 221 \times 3 \\ &= 391 \times 4 - 221 \times 7. \end{aligned}$$

つまり $(x, y) = (4, -7)$ は方程式 $391x + 221y = 17$ の一組の解となる.

以上の議論を一般の場合に拡張すれば次の定理が得られる.

定理 2.2 (拡張されたユークリッド互除法)**.** 整数 a, b $(ab \neq 0)$ に対し, 一次不定方程式

$$ax + by = \gcd(a, b)$$

には (少なくとも一つ) 解が存在する. その解はユークリッドの互除法を用いることにより, 具体的に与えられる.

2.2　一次不定方程式の解法

一般の一次不定方程式は解を持つとは限らない. 例えば方程式 $6x + 8y = 2$ は定理 2.2 により (あるいは, 拡張されたユークリッドアルゴリズムにより) 解 $(x, y) = (-1, 1)$ をもつ. 一方, 方程式

$$6x + 8y = 5$$

は整数解 (x, y) を持たない. 実際, 上の等式の左辺は $6x + 8y = 2(3x + 4y)$ と式変形できるので, 命題 1.3 により偶数である. 一方, この等式の右辺 5 は奇数であるため, 整数解 (x, y) が存在しない. 一次不定方程式の解の存在については, 次の定理が知られている.

定理 2.3. 一次不定方程式 $ax + by = c$ が解を持つためには, c が a と b の最大公約数 d の倍数になることが必要かつ十分である.

証明) (必要性)　ある整数 x_0, y_0 が $ax_0 + by_0 = c$ を満たすとすれば, 命題 1.3 により c は d の倍数になる. (十分性)　定理 2.2 により, 方程式 $ax + by = d$ の解 $(x, y) = (x_0, y_0)$ が存在する. すなわち $ax_0 + by_0 = d$ を満たすような整数 x_0 と y_0 が存在する. $c' = c/d$ とおき, この式の両辺を c' 倍すれば,

$$a(c'x_0) + b(c'y_0) = c$$

が成立する. すなわち, $(x, y) = (c'x_0, c'y_0)$ は一次不定方程式 (2.1) の一組の解となる. □

注意 2.4. とくに a, b が互いに素 (すなわち $\gcd(a, b) = 1$) ならば, 任意の整数 c に対し, 一次不定方程式

$$ax + by = c$$

は必ず解を持つ.

例題 2.5. 一次不定方程式 $12x + 21y = 15$ の一組の解 (x, y) を与えよ.

解答)　(Step 1)　$\gcd(12, 21) = 3$ であり, 方程式の右辺の 15 がその倍数であることから解が存在する. まず, ユークリッドの互除法により

$$12x + 21y = 3$$

の解を一つ与える. $21 = 12 \times 1 + 9$, $12 = 9 \times 1 + 3$ より,

$$3 = 12 - 9 \times 1 = 12 - (21 - 12 \times 1) \times 1 = 12 \times 2 + 21 \times (-1). \tag{2.7}$$

よって $x = 2$, $y = -1$ は $12x + 21y = 3$ の一つの解となる.
(Step 2)　(Step 1) の式 (2.7) の両辺を $5 = 15/3 (= c/d)$ 倍する. (ここで $c = 15$, $d = \gcd(12, 21) = 3$ である.)

$$3 \times 5 = 12 \times \underbrace{(2 \times 5)}_{=x} + 21 \times \underbrace{((-1) \times 5)}_{=y}.$$

以上より $(x, y) = (10, -5)$ は $12x + 21y = 15$ の一組の解である.

例題 2.6. 一次不定方程式 $12x + 21y = 15$ の全ての解 (x, y) を求めよ.

解答)　例題 2.5 により, $(x, y) = (10, -5)$ は $12x + 21y = 15$ の一組の解である. 一般解を (x, y) とすれば, 2 つの等式

$$\begin{cases} 12 \cdot x + 21 \cdot y & = 15 \\ 12 \cdot 10 + 21 \cdot (-5) & = 15 \end{cases}$$

を得る. 辺どうしで引き算をすると,

$$12(x - 10) + 21(y + 5) = 0$$

が成り立つ. 両辺を $\gcd(12, 21) = 3$ で割ると,

$$4(x - 10) + 7(y + 5) = 0$$

が成り立つ. ここで 4 と 7 は互いに素であることに注意すると,

$$\frac{x - 10}{7} = -\frac{y + 5}{4} = t$$

が整数となり, t は方程式の解全体の空間をパラメータ付ける. したがって求める解は

$$\begin{cases} x & = 7t + 10 \\ y & = -4t - 5 \end{cases} \qquad (\text{ただし } t \text{ は任意の整数})$$

となる.

以下に一次不定方程式の解法について整理する.

一次不定方程式 $ax+by=c$ の解法

Step 1. c が $\gcd(a,b)$ の倍数かどうかについてチェックする. Yes なら Step 2 へ進む. No なら「解なし」となる.

Step 2. $d:=\gcd(a,b)$ で方程式 $ax+by=c$ の両辺を割り算する.

$$a'=\frac{a}{d},\qquad b'=\frac{b}{d},\qquad c'=\frac{c}{d}$$

とおけば, 与えられた方程式は

$$a'x+b'y=c' \tag{2.8}$$

と同等になる.

Step 3. ユークリッドの互除法で, $a'x+b'y=1$ の一組の解 $(x,y)=(x_0,y_0)$ を与える. このとき $(x,y)=(c'x_0,c'y_0)$ は (2.8) の一組の解となる.

Step 4. したがって, 求める全ての解は

$$\begin{cases} x &= c'x_0+b't \\ y &= c'y_0-a't \end{cases} \qquad (\text{ただし } t \text{ は任意の整数}) \tag{2.9}$$

となる.

注意 2.7. 解 (2.9) において, a' と b' はどちらに負の符号 $(-)$ がついても良い. つまり,

$$\begin{cases} x &= c'x_0-b't \\ y &= c'y_0+a't \end{cases} \qquad (\text{ただし } t \text{ は任意の整数})$$

も全ての解を与える.

3 合同式

本節では整数の合同式について学ぶ.

3.1 合同式とその性質

定義 3.1. 整数 a,b と自然数 n に対し, $a-b$ が n の倍数であるとき, a と b は n **を法として合同である**といい,

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

と式で表す.

例 3.2. $23-2=7\times 3$ なので, $23\equiv 2 \pmod 7$, $48-13=5\times 7$ なので, $48\equiv 13 \pmod 7$, $-2-1=3\times -1$ なので, $-2\equiv 1 \pmod 3$ のように用いる.

合同式 $a\equiv b \pmod n$ は, 整数全体の間の同値関係を定義する.

命題 3.3. 自然数 n と整数 a,b,c に対し, 次が成り立つ:

(1) $a\equiv a \pmod n$. (反射律)

(2) $a \equiv b \pmod{n}$ ならば, $b \equiv a \pmod{n}$. (対称律)
(3) $a \equiv b \pmod{n}$ かつ $b \equiv c \pmod{n}$ ならば, $a \equiv c \pmod{n}$. (推移律)

証明は簡単なので, 各自で示して欲しい.

補題 3.4. 整数 a, a', b, b' と自然数 n に対し, $a \equiv a'$ かつ $b \equiv b' \pmod{n}$ ならば, 次が成り立つ:

(1) $a + b \equiv a' + b' \pmod{n}$
(2) $ab \equiv a'b' \pmod{n}$

すなわち, 整数の足し算 (引き算) と掛け算において, 等式と同じ性質が合同式にも成立していることがわかる.

証明) $a \equiv a'$ かつ $b \equiv b' \pmod{n}$ のとき, 合同式の定義より, $a - a' = kn$, $b - b' = ln$ を満たす整数 k, l が存在する. このとき

$$\begin{aligned}(a+b) - (a'+b') &= (a-a') + (b-b') \\ &= kn + ln \\ &= (k+l)n\end{aligned}$$

により, $a + b \equiv a' + b' \pmod{n}$ が従う. 同様に

$$\begin{aligned}ab - a'b' &= (ab - a'b) + (a'b - a'b') \\ &= (a-a')b + a'(b-b') \\ &= (kb + a'l)n\end{aligned}$$

により, $ab \equiv a'b' \pmod{n}$ を得る. □

例 3.5. 5 を法として, $7 \equiv 2$ かつ $3 \equiv 8$ であるが,

$$7 \times 3 - 2 \times 8 = 21 - 16 = 5$$

であり, $7 \times 3 \equiv 2 \times 8 \pmod{5}$ が成り立つ. 同様に $7 + 3 \equiv 2 + 8 \pmod{5}$ も成り立つ.

整数の合同式 $a \equiv b \pmod{n}$ が成り立つのは, a と b を n で割ったときの余りによって決定される.

命題 3.6. 整数 a, b と自然数 n に対し, a を n で割ったときの余りを r, b を n で割ったときの余りを s とする. このとき

$$a \equiv b \pmod{n} \Longleftrightarrow r = s$$

が成り立つ.

証明) 仮定より,

$$\begin{aligned}a &= nq_1 + r, \qquad 0 \leq r < n \\ b &= nq_2 + s, \qquad 0 \leq s < n\end{aligned}$$

を満たす整数 q_i $(i = 1, 2)$ が存在する.

$$a - b = n(q_1 - q_2) + r - s$$

より, $a-b$ が n の倍数ならば $r-s$ も n の倍数になる. 一方余りの定義により $|r-s|<n$ であるから, このことは $r-s=0$, すなわち $r=s$ を意味する. 逆に $r=s$ ならば, 上の式により $a\equiv b \pmod n$ が成り立つことは明らかである. □

任意の整数 a と自然数 n に対し, a を n で割ったときの余り r は明らかに a と合同である. 命題 3.6 より, 自然数 n を一つ固定すると, 任意の整数は 0 から $n-1$ までのただ一つの自然数 (つまり n で割り算をするときの余り) と合同であることがわかる.

定義 3.7. 整数 a と自然数 n に対し, a を n で割ったときの余り (整数) を

$$a \mod n$$

と表す.

命題 3.6 によって,

$$a\equiv b \pmod n \Longleftrightarrow (a \mod n)=(b \mod n)$$

が成り立つ.

例 3.8. 合同式では $23\equiv 51 \pmod 7$ が成立する. $23 \mod 7=2$ $(23=7\times 3+2)$ かつ $51 \mod 7=2$ $(51=7\times 7+2)$ であるので,

$$23 \mod 7=51 \mod 7$$

となる.

3.2 剰余計算

補題 3.4 と命題 3.6 によって, 2 つの整数の掛け算の余りを, 余りの掛け算のみで求めることができる. このような計算の方法を一般に**剰余計算**という.

例 3.9. $365=7\times 52+1$ より, $365 \mod 7=1$ である. 一方 $20=7\times 2+4$ より, $20 \mod 7=4$ である.

$$365\times 20\equiv 1\times 6=6 \pmod 7.$$

より

$$365\times 20 \mod 7=6.$$

問題 3.10. 2020 年 1 月 1 日は水曜日である. 20 年後の 2040 年の 1 月 1 日は何曜日か, 剰余計算を用いて求めよ.

解答) 一年は原則として 365 日からなるが, 4 年に 1 度, 西暦が 4 の倍数の年だけ閏年 (うるうどし) と呼ばれ一年が 366 日からなる. [*2] 閏年の分を勘定に入れて, 20 年後の元旦までの日数を計算すると

$$365\times 20+\underbrace{5}_{\text{閏年の分}}$$

[*2] 閏年のルールについては, グレゴリオ歴では次のルールで閏年を決めている:
(1) 西暦年が 4 で割り切れる年は (原則として) 閏年とする.
(2) ただし, 西暦年が 100 で割り切れる年は (原則として) 平年とする.
(3) ただし, 西暦年が 400 で割り切れる年は必ず閏年とする.
詳細については他の情報を当たって欲しい.

に等しい. これを 7 で割ったときの余りは,

$$365 \times 20 + 5 \equiv 1 \times 6 + 5 = 11 \equiv 4$$

より 4 に等しくなる. したがって, 2040 年の 1 月 1 日は日曜日になる計算である.

例題 3.11. 次の計算をせよ: (1)　$289 \times 673 \pmod{11}$　　(2)　$123456789 \pmod{9}$

解答)　(1) $289 \equiv 69 \equiv 3$ と $673 \equiv 13 \equiv 2$ により,

$$289 \times 673 \equiv 3 \times 2 = 6.$$

(2) $10 \equiv 1 \pmod 9$ より, $10^k \equiv 1 \pmod 9$. したがって

$$\begin{aligned} 123456789 &= 1 \times 10^8 + 2 \times 10^7 + 3 \times 10^6 + 4 \times 10^5 + 5 \times 10^4 + 6 \times 10^3 + 7 \times 10^2 + 8 \times 10^1 + 9 \times 10^0 \\ &\equiv 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 \\ &= 0 \pmod 9. \end{aligned}$$

4　剰余類

4.1　剰余類の定義

定義 4.1. n を自然数とする. 整数 a に対し, $\mathbb{Z}$ の部分集合 $R(a)$ を

$$R(a) = \left\{ x \in \mathbb{Z} \;\middle|\; x \equiv a \pmod n \right\}$$

によって定義し, $R(a)$ を a を含む (a が代表する) **剰余類** *(residue class)* という.

例 4.2. $n = 3$ とする. このとき,

$$\begin{aligned} R(0) &= \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\} \\ R(1) &= \{\dots, -8, -5, -2, 1, 4, 7, 10, \dots\} \\ R(2) &= \{\dots, -7, -4, -1, 2, 5, 8, 11, \dots\} \\ R(3) &= R(0) \\ R(4) &= R(1) \\ &\vdots \end{aligned}$$

となる.

命題 4.3. 自然数 n と整数 a, b に対し, 次は同値である.

(1) $b \equiv a \pmod n$.
(2) $b \in R(a)$.
(3) $R(b) = R(a)$

例 4.4. 例えば $n = 3$ のとき, $4 \equiv 7 \pmod 3$ なので, $R(4) = R(7)$ となる.

命題 3.6 と命題 4.3 により, 全ての整数 a は, $R(0)$ から $R(n-1)$ のうちのいずれかただ 1 つの剰余類に属すので次の命題が成り立つ.

命題 4.5. n を自然数とする. 整数全体の集合 $\mathbb{Z}$ は, 剰余類の非交差和 (disjoint union) として,

$$\mathbb{Z} = R(0) \sqcup R(1) \sqcup \cdots \sqcup R(n-1)$$

と表される. ただし $X = A \sqcup B$ は, $X = A \cup B$ かつ $A \cap B = \emptyset$ を表す.

例えば $n = 3$ のとき, $\mathbb{Z} = R(0) \sqcup R(1) \sqcup R(2)$ である. 整数全体は 3 の倍数と, 3 で割って 1 余る整数, 3 で割って 2 余る整数の 3 つのクラスに分類されることを意味する.

定義 4.6. 剰余類の集合 $\{R(a) \mid a \in \mathbb{Z}\}$ を $\mathbb{Z}/n\mathbb{Z}$ で表す.

命題 4.3 により

$$\mathbb{Z}/n\mathbb{Z} = \{R(0), R(1), \ldots, R(n-1)\}$$

となる.

4.2 剰余類の和と積

n を自然数とする.

定義 4.7. n を法とする剰余類 $R(a), R(b) \in \mathbb{Z}/n\mathbb{Z}$ に対し, 剰余類の和と差, 積を以下のように定義する:

$$R(a) + R(b) := R(a+b)$$
$$R(a)R(b) := R(ab)$$

定義 4.7 において, $R(a)$ と $R(b)$ の和と積は, 命題 3.6 により, 代表元 a, b の選び方に依存することなく定義される. すなわち $R(a) = R(a')$, $R(b) = R(b')$ となるような整数 a, b, a', b' に対し, $R(a+b) = R(a'+b')$ かつ $R(ab) = R(a'b')$ が成立する. 数学ではこれを**うまく定義されている** *(well-defined)* と表現する. 定義 4.7 の和と積の定義により, $\mathbb{Z}/n\mathbb{Z}$ には**環** *(ring)* の構造が入る.[*3]

定義 4.8. 剰余類の集合 $\mathbb{Z}/n\mathbb{Z}$ に定義 4.7 により和と積を定義した環を, (n を法とする)$\mathbb{Z}$ の**剰余類環**, **または剰余環** *(residue class ring)* と呼ぶ.

例 4.9. 剰余類環 $\mathbb{Z}/5\mathbb{Z} = \{R(0), R(1), R(2), R(3), R(4)\}$ における和と積の演算表を書くと以下のようになる. 以下では簡単のために $R(a) \in \mathbb{Z}/n\mathbb{Z}$ を単に a と表す.

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

表や定義からもわかるように, 剰余類環 $\mathbb{Z}/n\mathbb{Z}$ において, 任意の整数 a, b に対し,

$$R(a) + R(b) = R(b) + R(a), \qquad R(a)R(b) = R(b)R(a)$$

[*3] 代数学ではこのような 2 つの演算を持つ代数構造を一般に環と呼ぶが, 詳細については後続の科目の「代数学 2」で学ぶ.

が成り立つ. すなわち, $\mathbb{Z}/n\mathbb{Z}$ において和と積は順序を交換しても演算結果は不変である. この事実から $\mathbb{Z}/n\mathbb{Z}$ は**可換環** *(commutative ring)* と呼ばれる.

5　ファルマーの (小) 定理

n を自然数とする. 二項展開定理

$$(x+y)^n := x^n + nx^{n-1}y + \frac{n(n-1)}{2}x^{n-2}y^2 + \cdots + \binom{n}{k}x^{n-r}y^r + \cdots + nxy^{n-1} + y^n$$

において（二項）係数

$$\binom{n}{r} = \frac{n!}{k!(n-r)!}$$

について考える. n が素数 p のとき次の補題が成り立つ.

補題 5.1. 素数 p と整数 r $(0 < r < p)$ に対し,

$$\frac{p!}{r!(p-r)!} \equiv 0 \pmod{p}$$

が成り立つ.

左辺の式の分母に現れる自然数がいずれも p よりも小さいことから, 分母は p で割り切れない. 一方, 分子は p で割り切れることから補題 5.1 は従う. 実際, $p = 5, r = 2$ のときも

$$\frac{5!}{2!3!} = \frac{5\cdot 4\cdot 3\cdot 2\cdot 1}{2\cdot 1\cdot 3\cdot 2\cdot 1} = 10 = 2\cdot 5 \equiv 0 \pmod{5}$$

のように, 分子の 5 が最後まで生き残る. 上記の二項展開定理と組み合わせると次の補題を得る.

補題 5.2. 素数 p と整数 a, b に対し,

$$(a+b)^p \equiv a^p + b^p \pmod{p}$$

が成り立つ.

さて次が初等整数論でもっとも有名なフェルマーの (小) 定理である.

定理 5.3 (フェルマーの小定理)**.** 素数 p と整数 a に対し,

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

が成り立つ. さらに a と p が互いに素ならば $(\gcd(a,p) = 1)$,

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

が成り立つ.

証明) $a > 0$ の場合には数学的帰納法により証明される. $a = 1$ の場合は明らかである. $a-1$ の場合に正しいとすると, 帰納法の仮定から

$$a^p = (a-1+1)^p \equiv (a-1)^p + 1^p = a - 1 + 1 = a$$

が正しい. したがって $a > 0$ のときは $a^p \equiv a \pmod{p}$ が成り立つ. $a < 0$ のときは $a' = -a$ とおいて,

$$a'^p = (-a)^p = -a.$$

ここで p が奇素数ならば $(-a)^p = -a^p$ となり, 両辺に -1 をかけて $a^p = a$ を得る. p が 2 のときは, $-1 \equiv 1 \pmod{2}$ より $-a = a$. いずれにせよ $a^p = a$ を得る. $a = 0$ のときは明らか. $\gcd(a, p) = 1$ のときは, $a^p \equiv a \pmod{p}$ の両辺を a で割ることができて (後述), $a^{p-1} \equiv 1 \pmod{p}$ を得る. □

例 5.4. (1) $10^{100} \mod 13$ を計算する. まずフェルマーの小定理より,

$$10^{12} \equiv 1 \pmod{13}$$

がわかる. したがって,

$$10^{100} = (10^{12})^8 \cdot 10^4 \equiv 1^8 \cdot 10^4 = 10^4 \pmod{13}.$$

一方 $10^2 = (-3)^2 = 9$ より,

$$10^4 = (10^2)^2 \equiv 9^2 \equiv (-4)^2 = 16 \equiv 3 \pmod{13}.$$

したがって, $10^{100} \mod 13 = 3$ がわかる.

(2) $2^{2020} \pmod{2017}$ を計算する. 2017 は素数であるので, $2^{2017-1} = 2^{2016} \equiv 1 \pmod{2017}$ である. したがって,

$$2^{2020} = 2^{2016} \cdot 2^4 \equiv 1 \cdot 16 = 16 \pmod{2017}.$$

6 既約剰余類と逆元

6.1 既約剰余類

n を自然数とする. 剰余類 $R(a) \in \mathbb{Z}/n\mathbb{Z}$ に対し, a を $R(a)$ の**代表元**と呼ぶ. 一般に剰余類 $R(a)$ に対し, 代表元 a の取り方は無限個存在する. 実際 $b \equiv a \pmod{n}$ を満たす整数 b は全て $R(a)$ の代表元である. 整数 a に対し, n と互いに素であるという性質は, n の整数倍を a に加えても変わらない (命題 4.3 参照). したがって, 次の命題が成り立つ.

命題 6.1. 整数 a に対し, 次は同値である.

(1) a は n と互いに素である.
(2) $R(a)$ に属する任意の整数 c は n と互いに素である.

つまり n を法とする剰余類には,

- 含まれるすべての整数が n と互いに素である剰余類と,
- 含まれるすべての整数が n と互いに素でない剰余類

の二種類が存在する. 前者は既約剰余類と呼ばれる.

定義 6.2. a を整数とする. a が n と互いに素であるとき, a を含む剰余類 $R(a)$ を (n を法とする) **既約剰余類** *(reduced residue class)* と呼ぶ.

例 6.3. $n = 12$ のとき, 1 から n までの整数のうち, n と互いに素であるものは $1, 5, 7, 11$ の 4 つである. したがって, 12 を法とする $\mathbb{Z}$ の既約剰余類は $R(1), R(5), R(7), R(11)$ の 4 つである.

6.2 逆元

数の体系や, より一般に (二項) 演算 $*$ が定義された集合 (マグマ)M において M の元 e が**単位元**であるとは, e が任意の $x \in M$ に対し,

$$x * e = e * x = x$$

を満たすことをいう. すなわち M のいかなる元 x も単位元 e との結合の影響を受けない. 一般には単位元 e は演算 $*$ によって異なる. 加法 $(+)$ と乗法 $(*)$ に関し任意の元 x に対し

$$x + 0 = 0 + x = x \qquad と \qquad x * 1 = 1 * x = x$$

を満たす 0 と 1 をそれぞれ**加法単位元**と**乗法単位元**と呼ぶ. 単位元が決まると, 逆元が定義される.

定義 6.4. 代数系 M において,

$$x + (-x) = (-x) + x = 0 \qquad と \qquad x * x^{-1} = x^{-1} * x = 1$$

を満たす $-x$ と x^{-1} をそれぞれ**加法逆元**と**乗法逆元**という.

(群以外の) 代数系では必ずしも乗法逆元は存在するとは限らない. 本節では剰余類の演算における乗法逆元の存在について取り扱う. 4.2 節では自然数 n に対し, n を法とする剰余類の集合 $\mathbb{Z}/n\mathbb{Z} = \{R(0), R(1), \dots R(n-1)\}$ において, 通常の整数の和と積を $\mod n$ で考えることにより, 剰余類の集合にも自然に和と積が定義され, $\mathbb{Z}/n\mathbb{Z}$ を**剰余類環**と呼ぶことを学んだ (定義 4.7 参照).

剰余類環 $\mathbb{Z}/n\mathbb{Z}$ において, n の倍数の定める剰余類 $R(0)$ と n で割ったとき余りが 1 に等しい整数の定める剰余類 $R(1)$ を考える. $\mathbb{Z}/n\mathbb{Z}$ の演算は可換であり, 任意の $R(a)$ に対し

$$R(0) + R(a) = R(a), \qquad R(1)R(a) = R(a)$$

が成り立つので, $R(0)$ と $R(1)$ はそれぞれ $\mathbb{Z}/n\mathbb{Z}$ における加法単位元と乗法単位元になる.

定義 6.5. 整数 n を法とする剰余類 $R(a)$ に対し,

$$R(a) \cdot R(b) = R(1)$$

を満たす剰余類 $R(b) \in \mathbb{Z}/n\mathbb{Z}$ を $R(a)$ の**乗法逆元**と呼び, 記号 $R(a^{-1})$ で表す. また

$$R(a^{-1}) = R(b) \qquad かつ \qquad 1 \leq b \leq n-1$$

を満たす整数 b を記号 $a^{-1} \mod n$ で表す.

注意 6.6. $R(a) \in \mathbb{Z}/n\mathbb{Z}$ に対し, その乗法逆元 $R(a^{-1}) \in \mathbb{Z}/n\mathbb{Z}$ はただ一通りに定まる. 実際, $R(a)R(b) = R(a)R(b') = R(1)$ とすると, $\mathbb{Z}/n\mathbb{Z}$ において積は可換であるので,

$$R(b) = R(b)R(1) = R(b)R(a)R(b') = R(1)R(b') = R(b')$$

となる. $R(a^{-1})$ は $R(1)$ から $R(n-1)$ のうちのいずれかただ一つと等しいので, 整数 $a^{-1} \mod n$ もただ一通りに定まる.

命題 3.6 により, $\mathbb{Z}/n\mathbb{Z}$ と n で整数を割った時の余りの集合 $\{0, 1, \dots, n-1\}$ の間には自然な一対一対応が存在する. 考えている元が $\mathbb{Z}/n\mathbb{Z}$ であるとわかれば, 元 $R(a)$ を a と表しても特に混乱は生じないので, 以下で

は記号の簡略化のために記号を乱用し, 剰余類 $R(a)$ $(0 \leq a \leq n-1)$ のことを代表元 a で表すことにする. すなわち,

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$$

と表す.

例 6.7. (1) $\mathbb{Z}/5\mathbb{Z} = \{0,1,2,3,4\}$ において,

$$2 \cdot 3 \equiv 1 \pmod 5 \quad \text{と} \quad 4^2 \equiv 1 \pmod 5$$

が成り立つので 2 と 3 は互いの逆元 (すなわち $2^{-1} \mod 5 = 3$ と $3^{-1} \mod 5 = 2$) であり, $4^{-1} \mod 5 = 4$ である.

(2) $\mathbb{Z}/4\mathbb{Z} = \{0,1,2,3\}$ において, $1, 3$ は逆元が存在するが, $2, 0$ については逆元が存在しない. ($\mathbb{Z}/4\mathbb{Z}$ の乗法演算表を書いて確認せよ.)

命題 6.8. n を自然数とし, a を $\mathbb{Z}/n\mathbb{Z}$ の元とする. a の乗法逆元 a^{-1} が存在するためには, a が既約剰余類であることが必要十分である.

証明) (必要性)　a の乗法逆元 $a^{-1} \mod n$ が存在すると仮定する. このとき $ax \equiv 1 \pmod n$ を満たす整数 $1 \leq x \leq n-1$ が存在する. すなわち $ax - 1$ が n の倍数となり, 一次不定方程式 $ax + ny = 1$ が整数解 (x, y) を持つ. このとき定理 2.3 により, $\gcd(a, n) = 1$ となる.
(十分性)　a と n が互いに素とする. 定理 2.3 により, $ax + ny = 1$ を満たす整数 x, y が存在する. 両辺の $\mod n$ を取れば, $a(x \mod n) \equiv 1 \pmod n$ が得られる. したがって, $b = x \mod n$ とおけば, $1 \leq b \leq n$ であり, $ab \equiv 1 \pmod n$ を満たすので, $b \in \mathbb{Z}/n\mathbb{Z}$ は a の乗法逆元となる. □

一般の可換環 R において, このように乗法逆元を有す元を**正則元** *(unit)* という.

例 6.9. 剰余類環 $\mathbb{Z}/6\mathbb{Z} = \{0,1,2,3,4,5\}$ において, 既約剰余類は $1, 5$ である. 一方, $0, 2, 3, 4$ は逆元を持たない.

命題 6.8 の証明からも分かる通り, 与えられた $a \in \mathbb{Z}/n\mathbb{Z}$ に対しその乗法逆元 $a^{-1} \mod n$ を求めることは, 一次不定方程式 $ax + ny = 1$ を解くことに他ならない. 以下では 2 通りの乗法逆元の計算例を紹介する.

例題 6.10. $\mathbb{Z}/11\mathbb{Z}$ において, 9 の乗法逆元 $9^{-1} \mod 11$ を計算せよ.

解法 1)　9 の倍数を次々に考えて, 11 で割った余りが 1 に等しいものを探す:

x	1	2	3	4	5	$\cdots$
$9x$	9	18	27	36	45	$\cdots$
$9x \mod 11$	9	7	5	3	1	$\cdots$

上の表により $9 \times 5 = 45 = 4 \times 11 + 1 \equiv 1 \pmod{11}$ であるので, 9 の乗法逆元は 5 であることがわかる.
解法 2)　一次不定方程式 $9x + 11y = 1$ の解を求める. 11 と 9 に (拡張された) ユークリッドの互除法 (定理 1.11) を適用すると, $11 = 9 \times 1 + 2$, $9 = 2 \times 4 + 1$ となり, これらの式から,

$$1 = 9 - 2 \times 4 = 9 - (11 - 9) \times 4 = 9 \times 5 - 11 \times 4,$$

すなわち, 一つの解として $x = 5$, $y = -4$ が得られる. したがって, $9 \times 5 \equiv 1 \pmod{11}$. 9 の乗法逆元はやはり 5 である.

命題 6.11. $\mathbb{Z}/n\mathbb{Z}$ の既約剰余類全体は, 乗法と逆元に関して閉じている, すなわち a, b が共に既約剰余類ならば, ab および a^{-1} も既約剰余類である.

注意 6.12. $\mathbb{Z}/n\mathbb{Z}$ の既約剰余類の集合を $(\mathbb{Z}/n\mathbb{Z})^\times$ と表す. 命題 6.11 の主張は, $(\mathbb{Z}/n\mathbb{Z})^\times$ が乗法に関して群をなすということを主張するものである. $(\mathbb{Z}/n\mathbb{Z})^\times$ を $\mathbb{Z}/n\mathbb{Z}$ の**既約剰余類群** *(reduced residue class group)* と呼ぶ.

例 6.13. 例 6.3 より, 12 を法とする既約剰余類群 $(\mathbb{Z}/12\mathbb{Z})^\times$ は集合として $\{1, 5, 7, 11\}$ と表せる.

7　一次合同式

自然数 n と整数 a, b に対し, x を未知数とする方程式

$$ax \equiv b, \qquad a \not\equiv 0 \pmod{n} \tag{7.1}$$

を**一次合同式**という. この方程式を満たす整数解 x を求めることを, "一次合同式を解く" という. 整数 x が一次合同式 (7.1) を満たすとき, x に n の整数倍を加えたものもすべて (7.1) を満たす. そのため (7.1) に解が存在するとき, その (一般) 解は

$$x \equiv a_1, \ldots, a_k \pmod{n}$$

のように表される. したがって, 一次合同式の「解の個数」という場合には, (7.1) を満たす n を法とする剰余類 $R(a_1), \ldots, R(a_k)$ の個数 k を表すものとする. 以下では一次合同式の解の存在と解の個数について考える.

7.1　一意解を持つ場合

まずもっとも単純な場合について取り扱う. n を法とする $\mathbb{Z}$ の剰余類 $R(a)$ に対し, その (乗法) 逆元が存在するためには, 命題 6.8 より a と n が互いに素であることが必要十分である. したがって a と n が互いに素であるとき, 式 (7.1) の両辺に逆元 $a^{-1} \mod n$ を乗じて,

$$x = a^{-1}ax \equiv a^{-1}b \pmod{n}$$

と (7.1) の解はただ一つ存在する.

命題 7.1. a, b を整数とし n を自然数とする. a と n が互いに素ならば, 一次合同式 (7.1) はただ一つの解をもち, 解は

$$x \equiv a^{-1}b \pmod{n}$$

で与えられる.

例 7.2.　(1) $9x \equiv 8 \pmod{11}$ を考える. $9^{-1} \mod 11 = 5$ (実際, $9 \times 5 = 45 \equiv 1 \pmod{11}$ が成り立つ) より, 解は

$$x = 9^{-1} \cdot 9 = 5 \cdot 8 = 40 \equiv 7 \pmod{11}$$

と求められる.

(2) $12x \equiv 3 \pmod{29}$ を考える. ユークリッドの互除法を用いて $12^{-1} \mod 29$ を計算すると $12^{-1} \mod 29 = 17$ とわかる. したがって

$$x = 12^{-1} \cdot 3 = 17 \cdot 3 = 51 \equiv 22 \pmod{29}$$

と解がただ一つ存在する.

7.2　複数解を持つ場合, または解が存在しない場合

次に a と n が互いに素でない場合について取り扱う. 整数 x が一次合同式 (7.1) を満たすことは, 整数 y が存在し, x, y が一次不定方程式

$$ax + ny = b \tag{7.2}$$

を満たすことと同値である. a と n の最大公約数 $\gcd(a, n)$ を d により表せば, 定理 2.3 により方程式 (7.2) に整数解 x, y が存在するためには, b が d の倍数になることが必要十分である. またこのとき (7.2) の一つの解を (x_0, y_0) と表せば, 求めるすべての解 (x, y) は $n' = n/d$ と $a' = a/d$ に対し, $x = x_0 + n't$, $y = y_0 - a't$ $(t \in \mathbb{Z})$ と表される (2.2 節参照). したがって, 次の定理を得る.

定理 7.3. 一次合同式 (7.1) が解を持つためには $d = \gcd(a, n)$ が b を割り切ることが必要十分条件である. また (7.1) の一つの解を $x = x_0$ とすれば, 一般解は

$$x \equiv x_0 + (n/d)t \pmod{n} \qquad (t = 0, 1, 2, \ldots, d-1)$$

と表される. とくに解の個数は d に等しい.

例 7.4.　(1) 一次合同式 $14x \equiv 20 \pmod{35}$ を考える. 式の右辺の 20 は $\gcd(14, 35) = 7$ の倍数でない. したがってこの一次合同式には解が存在しない.

(2) 一次合同式 $14x \equiv 21 \pmod{35}$ を考える. 式の右辺の 21 は $\gcd(14, 35) = 7$ の倍数であるので, この一次合同式には解が存在する.

$$14x \equiv 21 \pmod{35} \Longleftrightarrow 2x \equiv 3 \pmod{5}$$

より, $x \equiv 4 \pmod 5$ が一つの解である. 解 x を mod 35 で考えれば, 求める解は $x \equiv 4, 9, 14, 19, 24, 29, 34 \pmod{35}$. すなわち与えられた一次合同式には 35 を法として, 解は 7 個存在する.

一次合同式 $ax \equiv b \pmod n$ の解法

n が自然数, a, b は整数とする.

Step 1. $d = \gcd(a, n)$ を求め, b が d の倍数かどうかをチェックする. Yes なら Step 2 へ進む. No なら「解なし」となる.

Step 2. $a' = \dfrac{a}{d}, n' = \dfrac{n}{d}, b' = \dfrac{b}{d}$ とおいて, 一次合同式

$$a'x \equiv b' \pmod{n'}$$

の解 $x_0' \pmod{n'}$ を求める. (解 $x = x_0'$ は n' を法としてただ一つ存在する.)

Step 3. 求める解は,

$$x \equiv x_0', x_0' + n', x_0' + 2n', \ldots, x_0' + (d-1)n' \pmod{n}$$

となる (解の個数は d になる).

7.3　中国剰余定理 (連立合同式)

m と n を 2 つの整数とする. m と n の最大公約数 $\gcd(m,n)$ が 1 に等しいとき m **と** n **は互いに素である**という.

定理 7.5 (中国剰余定理)**.** m と n を互いに素な 2 つの整数とする. 任意の整数 a, b に対し, 連立合同式

$$\begin{cases} x & \equiv a \pmod{m} \\ x & \equiv b \pmod{n} \end{cases}$$

の解は積 mn を法として唯 1 つ存在する.

中国剰余定理 (Chinese Remainder Theorem) は中国の数学書「孫子算経」の問題「3 で割ると 2 余り, 5 で割ると 3 余り, 7 で割ると 2 余る数を求めよ. 」に由来がある.

定理 7.6. $m_1, \ldots, m_r$ は互いに素な r 個の整数とする. 任意の整数 $a_1, \ldots, a_r$ に対し, 連立合同式

$$\begin{cases} x & \equiv a_1 \pmod{m_1} \\ x & \equiv a_2 \pmod{m_2} \\ & \vdots \\ x & \equiv a_r \pmod{m_r} \end{cases} \tag{7.3}$$

の解は $M := m_1 \cdots m_r$ を法として, 唯 1 つ存在する.

整数の組 $(a_1, \ldots, a_r)$ が与えられれば, 解 x を以下の手順に従って, 求めることが可能である.

連立合同方程式 (7.3) の解法

Step 1. 各 i に対し, $m_1, \ldots, m_r$ から m_i を除いた積

$$M_i := \frac{M}{m_i} = m_1 \cdots \widehat{m_i} \cdots m_r \mod m_i$$

を $\mod m_i$ で求める.

Step 2. 各 i に対し, 合同方程式

$$M_i t_i \equiv 1 \pmod{m_i} \tag{7.4}$$

を解く. (M_i と m_i は互いに素であるため, 一意解が存在する.)

Step 3.

$$x = a_1 M_1 t_1 + a_2 M_2 t_2 + \cdots + a_r m_r t_r \pmod{M}$$

が求める解である.

これが連立合同方程式 (7.3) を満たすことは次のようにしてわかる. 各 j に対し M_j は $m_i (i \neq j)$ を約数に持つ. よって, $j \neq i$ に対し, $M_j \equiv 0 \pmod{m_i}$. 式 (7.4) より,

$$x \equiv 0 + \cdots + a_i \cdot 1 + \cdots + 0 = a_i \pmod{m_i}$$

となる.

例題 7.7. 連立合同方程式

$$\begin{cases} x & \equiv a_1 \pmod 2 \\ x & \equiv a_2 \pmod 3 \\ x & \equiv a_3 \pmod 7 \end{cases}$$

の解を求めよ.

解答)

$$\begin{aligned} 3 \cdot 7t_1 &\equiv 1 \pmod 2 \\ 2 \cdot 7t_2 &\equiv 1 \pmod 3 \\ 2 \cdot 3t_3 &\equiv 1 \pmod 7 \end{aligned}$$

の解を求めると $t_1 \equiv 1 \pmod 2$, $t_2 \equiv 2 \pmod 3$, $t_3 \equiv -1 \pmod 7$. よって求める連立合同方程式の解は

$$\begin{aligned} x &= a_1 \cdot 21 \cdot t_1 + a_2 \cdot 14 \cdot t_2 + a_3 \cdot 6 \cdot t_3 \\ &= 21a_1 \cdot 1 + 14a_2 \cdot 2 + 6a_3 \cdot -1 \\ &= 21a_1 + 28a_2 - 6a_3 \pmod{42}. \end{aligned}$$

例えば, $a_1 = 1, a_2 = 2, a_3 = 6$ のときは, $x \equiv 21 + 56 - 36 = 41 \pmod{42}$ となる.

8 オイラーの定理

8.1 オイラー関数とオイラーの公式

定義 8.1. 自然数 n に対し $\{1, \ldots, n\}$ の中で n と互いに素となる数の個数を $\varphi(n)$ を対応させる関数 $n \mapsto \varphi(n)$ を**オイラー関数**という.

例 8.2. $n = 1$ から $n = 12$ までのオイラー関数の値 $\varphi(n)$ を計算すると以下の表のようになる.

n	1	2	3	4	5	6	7	8	9	10	11	12	$\cdots$
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	$\cdots$

自然数 n を法とする任意の剰余類 $R(a)$ の代表元 a は, 0 から $n-1$ までの整数を取ることができるので, 次の命題が成り立つ.

命題 8.3. 自然数 n に対しオイラー関数の値 $\varphi(n)$ は, $\mathbb{Z}/n\mathbb{Z}$ における既約剰余類の個数に等しい.

以下にオイラー関数の性質をまとめる.

命題 8.4. (1) 任意の自然数 e と任意の素数 p に対し,

$$\varphi(p^e) = p^e - p^{e-1}$$

が成り立つ.

(2) 互いに素な自然数 a, b に対し,

$$\varphi(ab) = \varphi(a)\varphi(b)$$

が成り立つ (オイラー関数の乗法性).

(3) 自然数 n の素因数分解が

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

と得られたとする．ただし p_i $(1 \leq i \leq k)$ は n の相異なる素因数とし, e_i $(1 \leq i \leq k)$ は自然数とする．このとき

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

が成り立つ．

証明) p^e 以下の自然数のうち p の倍数となるものの個数が p^{e-1} に等しいことから (3) がわかる．(2) は少し議論を要すが, 中国剰余定理を用いることで証明される．(3) は n の素因数分解に (1) とオイラー関数の乗法性 (2) を用いることで証明される． □

例 8.5. $360 = 2^3 \cdot 3^2 \cdot 5$ なので

$$\varphi(360) = 360 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = \frac{360 \cdot 1 \cdot 2 \cdot 4}{2 \cdot 3 \cdot 5} = 96.$$

つまり $\mathbb{Z}/360\mathbb{Z}$ において既約剰余類の個数は 96 に等しいことがわかる．

8.2 オイラーの定理

次が有名なオイラーの定理で, フェルマーの小定理 (定理 5.3) の一般化となっている．

定理 8.6 (オイラーの定理)**.** φ をオイラー関数とする．自然数 n と整数 a に対し, a と n が互いに素ならば,

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

が成り立つ．

証明) n を法とする既約剰余類群を $(\mathbb{Z}/n\mathbb{Z})^\times = \{a_1, \ldots, a_n\}$, ただし $1 \leq a_i \leq n-1$ $(1 \leq i \leq m)$ とする．このとき, 命題 8.3 により, $m = \varphi(n)$ が成り立つ．n と互いに素な整数 a に対し, $X := (\mathbb{Z}/n\mathbb{Z})^\times$ 上の a 倍写像

$$\psi : X \longrightarrow X, \qquad b \mapsto a * b$$

を考える．a は既約剰余類に属すので, 命題 6.8 より a の乗法逆元 $a^{-1} \mod n$ が存在する．したがって ψ は単射であり, ψ が X 自身への写像であることから全単射になる $(\psi(X) = X)$．つまり ψ の像

$$\psi(X) = \{\psi(a_1), \ldots, \psi(a_m)\}$$

は X に一致し, $\psi(a_1), \ldots, \psi(a_m)$ は $a_1, \ldots, a_m$ を並べ替えただけとなる．したがって, $\mathbb{Z}/n\mathbb{Z}$ において

$$\begin{aligned} a_1 \cdots a_m &= \psi(a_1) \cdots \psi(a_m) \\ &= (aa_1) \cdots (aa_m) \\ &= a^m \cdot (a_1 \ldots a_m) \end{aligned}$$

が成り立つ．ここで各 a_i $(1 \leq i \leq m)$ は既約剰余類であり, 乗法逆元が存在する (命題 6.8)．式の両辺を $a_1 \cdots a_m$ で割ると, $\mathbb{Z}/n\mathbb{Z}$ における等式 $a^m = 1$ を得る．$m = \varphi(n)$ より, オイラーの定理の主張が従う． □

例 8.7. $11^{100} \mod 28$ を計算する．$28 = 2^2 \times 7$ より, $\varphi(28) = 28(1 - 1/2)(1 - 1/7) = 12$．まずオイラーの定理より, $11^{12} \equiv 1 \pmod{28}$ がわかる．したがって,

$$11^{100} = 11^{12 \times 8 + 4} = (11^{12})^8 \cdot 11^4 \equiv 11^4 \pmod{28}$$

と求められる．$11^2 = 121 \equiv 9$ かつ $9^2 = 81 \equiv 25$ より, $11^{100} \mod 28 = 25$ となる．

9　位数と原始根

9.1　位数

定義 9.1. 自然数 n と n と互いに素な整数 a に対し,

$$a^s \equiv 1 \pmod{n}$$

を満たす最小の自然数 s を, 法 n に関する a の**位数** *(order)* といい, 記号 $\mathrm{ord}_n(a)$ で表す.

例 9.2. 法 13 に関する $a = 2$ の位数を計算する.

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 8 \cdot 2 = 16 \equiv 3, \quad 2^5 \equiv 3 \cdot 2 = 6, \quad 2^6 \equiv 6 \cdot 2 = 12 \equiv -1$$

となり, 一方,

$$2^7 = 2^6 \cdot 2 \equiv -2, \quad 2^8 \equiv -4, \quad 2^9 \equiv -8, \quad 2^{10} \equiv -3, \quad 2^{11} \equiv -6, \quad 2^{12} \equiv 1$$

となる. したがって $2^1, \ldots, 2^{11}$ まではすべて 1 と合同でなく, 2^{12} ではじめて 1 と合同になる. したがって法 13 に関する 2 の位数は 12 に等しい. 同様に $a = 1, \ldots, 12$ に対し, 法 13 に関する a の位数を計算すると以下の表のようになる:

$\mathbb{Z}/13\mathbb{Z}$ の元	1	2	3	4	5	6	7	8	9	10	11	12
位数	1	12	3	6	4	12	12	4	6	6	12	2

$2, 6, 7, 11$ が最大位数 12 をもち, 他の元の位数はすべて 12 の約数になることに注意したい. じつは, これらの最大位数をもつ元は" 原始根" と呼ばれ, 次節 9.2 節で詳しく学ぶ.

命題 9.3. 自然数 n と n と互いに素な整数 a に対し, n に関する a の位数を s とする.

(1) n を法として, $1, a, a^2, \ldots, a^{s-1}$ はどの 2 つも互いに合同でない.
(2) $a^m \equiv 1 \pmod{n}$ ならば, m は s の倍数である.
(3) $\varphi(n)$ は s の倍数である.

証明) (1) $a^i \equiv a^j \pmod{n}$, $1 \leq i \leq j \leq s-1$ とする. a は n と互いに素であるため, 乗法逆元 a^{-1} が存在し, 両辺に a^{-i} を乗じると, $a^{j-i} \equiv 1 \pmod{n}$ を得る. $0 \leq j - i \leq s-1$ より, 位数の定義から $i = j$ が従う.
(2) m を s で割ったときの商を q とし, 余りを r とすると,

$$1 \equiv a^m = a^{qs+r} = (a^s)^q \cdot a^r \equiv 1^q \cdot a^r = a^r \pmod{n}$$

が成り立つ. 余りの定義により, $0 \leq r < s$ であり, 再び位数の定義から $r = 0$, すなわち m は s で割り切れる.
(3) オイラーの定理より, $a^{\varphi(n)} \equiv 1 \pmod{n}$ となる. 主張 (2) より, $s | \varphi(n)$ がわかる. □

9.2　原始根

以下では p を素数とする.

定義 9.4. 法 p に関する位数が $p-1$ に等しい整数 a を, p を法とする**原始根** *(primitive root)* という.

命題 9.3 より, p を法とするとき, 各元の位数は $\varphi(p) = p-1$ の約数である. すなわち原始根とは, 最大の位数 $p-1$ を持つ p で割り切れない整数ということになる.

例 9.5. 例 9.2 では, 法 $p = 13$ に関する元の位数を求めた. 位数が 12 $(= p-1)$ の元は,

$$2, 6, 7, 11$$

であり, これらの整数が 13 を法とする原始根である. 同様に法 11 に関して位数 10 の元を求めると

$$2, 6, 7, 8$$

となることがわかる. つまりこれらの整数が 11 を法とする原始根である.

p を法とする原始根 a がひとつ与えられると, 命題 9.3(1) により, $p-1$ 個の整数 $1, a, \ldots, a^{p-2}$ はどの 2 つも互いに合同でない. したがってこれらの定める集合は, $(\mathbb{Z}/p\mathbb{Z})^\times = \{1, \ldots, p-1\}$ 全体と一致する. すなわち任意の j $(1 \leq j \leq p-1)$ に対し,

$$j \equiv a^i \qquad \text{かつ} \qquad 0 \leq i \leq p-2$$

を満たす整数 i がただひとつ存在する. したがって, 法 p に関する剰余類の集合 $\mathbb{Z}/p\mathbb{Z}$ は

$$\mathbb{Z}/p\mathbb{Z} = \left\{0, 1, a, \ldots, a^{p-2}\right\}$$

と表せる. このような原始根 a のべきを用いた $\mathbb{Z}/p\mathbb{Z}$ の元の表し方を (有限体 $\mathbb{Z}/p\mathbb{Z}$ の) **べき表現**という.

例 9.6. $\mathbb{Z}/11\mathbb{Z}$ において 2 の位数は 10 に等しい. したがって 2 は 11 を法とする原始根である. 原始根 2 に関するべき表現を以下の表に記す.

$\mathbb{Z}/11\mathbb{Z}$ の元	1	2	3	4	5	6	7	8	9	10
べき表現	2^0	2^1	2^8	2^2	2^4	2^9	2^7	2^3	2^6	2^5

有限体 $\mathbb{Z}/p\mathbb{Z}$ において, 積を計算するときはべき表現を用いて計算すると便利である. 一方, 和を計算するときは通常の表記 (p で割ったときの剰余 $0, 1, \ldots, p-1$) を用いて計算するのが便利なので, 上記のような対応表がよく用いられる.

命題 9.7. (1) 自然数 n に関する整数 a の位数を s とする $(\mathrm{ord}_n(a) = s)$. このとき,

$$\mathrm{ord}_n(a^t) = \frac{s}{\gcd(s, t)}$$

が成り立つ.

(2) a を法 p に関する原始根とする. このとき,

$$\mathrm{ord}_p(a^t) = \frac{p-1}{\gcd(p-1, t)}$$

が成り立つ. とくに t と $p-1$ が互いに素であれば, a^t は法 p に関する原始根である.

例 9.8. 例 9.5 で見たように, 法 $p = 11$ に関する 2 の位数は 10 であり, 2 は 11 を法とする原始根である. 一方, 例 9.6 より, 法 $p = 11$ のもとで, $6, 7, 8$ はそれぞれ $6 = 2^9, 7 = 2^7, 8 = 2^3$ とべき表現を用いて表される. これらのべき表現において, $2^9, 2^7, 2^3$ の指数 $9, 7, 3$ は $p - 1 = 10$ と互いに素であるから, 命題 9.7 により, $\mathbb{Z}/11\mathbb{Z}$ において $6, 7, 8$ も原始根である. この事実は, 例 9.5 の事実と符合する. また命題 9.7 を用いて, $\mathbb{Z}/11\mathbb{Z}$ の各元の位数を求めると

$\mathbb{Z}/11\mathbb{Z}$ の元	1	2	3	4	5	6	7	8	9	10
べき表現	2^0	2^1	2^8	2^2	2^4	2^9	2^7	2^3	2^6	2^5
位数	1	10	5	5	5	10	10	10	5	2

となる.

一般に与えられた素数 p に対し, 手計算により原始根を探すのは難しい[*4]が, 与えられた整数が原始根かどうかは次の判定法により容易に判定することが可能である.

命題 9.9 (原始根判定法)**.** p を素数とし, a を整数とする. $p-1$ の素因数分解

$$p-1=\prod_{i=1}^{k} p_i^{m_i}$$

に現れるすべての素因数 p_i $(i=1,\dots,k)$ に対し

$$a^{(p-1)/p_i} \not\equiv 1 \pmod{p}$$

ならば, a は p を法とする原始根である.

証明) 命題 9.3(3) により, a の位数 s は $\varphi(p)=p-1$ の約数である. もし a が原始根でなければ, s は $p-1$ の真の約数となり, したがって, 適当な $i=1,\dots,k$ が存在し, $(p-1)/p_i$ が s で割り切れる, すなわち, $(p-1)/p_i=ks$ となるような自然数 k が存在する. このとき,

$$a^{(p-1)/p_i}=a^{ks}=(a^s)^k\equiv 1 \pmod{p}$$

が成り立つ. □

例 9.10. (1) $p=31$ は素数である. $p-1=31-1=2\cdot 3\cdot 5$ と素因数分解される. $3^3=27=-4 \pmod{31}$ より,

$$3^{30/2}=3^{15}=(3^3)^5\equiv(-4)^5=-2^{10}=-(2^5)^2\equiv -1^2=-1\not\equiv 1 \pmod{31}.$$

同様に $3^{30/3}=3^{10}=25\not\equiv 1 \pmod{31}$ と $3^{30/5}=3^6=16\not\equiv 1 \pmod{31}$ がわかる. したがって命題 9.9 より 3 は 31 を法とした原始根である[*5].

(2) $p=2017$ は素数である. $p-1=2016=2^5\cdot 3^2\cdot 7$ と素因数分解される.

$$5^{2016/2}=5^{1008}\equiv 2016\equiv -1 \pmod{2017}.$$

同様に $5^{2016/3}=5^{672}\equiv 294\not\equiv 1 \pmod{2017}$ と $5^{2016/7}=5^{288}\equiv 1879\not\equiv 1 \pmod{2017}$ がわかる. したがって命題 9.9 より 5 は 2017 を法とした原始根である[*6].

定理 9.11. 任意の素数 p に対し, p を法とする原始根が存在する.

[*4] Mathematica (本原稿執筆時の ver.12.0.0.0) のコマンドの “PrimitiveRootList” を用いると, 一瞬で原始根のリストを出してくれる.

[*5] $p=31$ を法とした原始根のリストは $3, 11, 12, 13, 17, 21, 22, 24$ となる.

[*6] $p=2017$ を法とした原始根のリストは $5, 10, 15, 19, 20, 26, 30, 35, 37, 38, 43, 47, 51, 52, 53, 59, 60, 67, 70, 80, 86, 94, 97, \dots, 2012$ となり, 全部で 576 個存在する.

証明) 証明については, [1, 定理 5.4.3] を参照して欲しい. □

Acknowledgement 本講義ノートは以下の書籍・文献を参考に書かれている. 本講義を受け, 初等整数論に関心をもった学生は続けて以下の本を読むことをお勧めしたい.

参考文献

[1] 楫元, 工科系のための初等整数論入門, 培風館, 2000.
[2] 植松友彦, 代数系と符号理論, オーム社, 2010.
[3] 萩田真理子, 暗号のための代数入門, サイエンス社, 2010.