演算の数理 講義まとめ

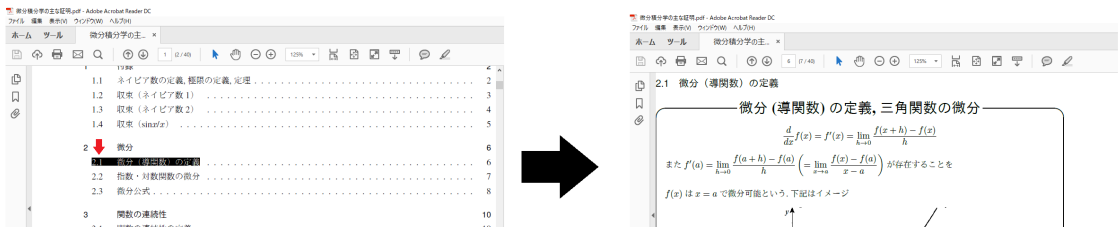
最終更新日：2019 年 2 月 11 日

はじめに

これは大学 2 年次の演算の数理 I, II の講義で学習した定義・定理を（証明なども含め）簡単にまとめたものです． 多少タイプミス等があるかもしれませんが， ご了承ください．すべての内容が収録されているわけではありませんが，復習などご自由に役立ててください．この PDF を作った人は，高校生の時，非常に整数の単元が苦手だったため，できる限り，わかりやすくまとめているつもりです．線型代数の基礎知識があれば，高校生でも理解できるようなまとめかたをしているつもりですので，気楽に読み進めることができると思います． 目次の行きたい単元の頭番号を押すとそのページへ行けます.(下記参照)

本 PDF では，ベクトル表示は $\mathfrak{a}$，実数，複素数，自然数全体の集合等を $\mathbb{R}$, $\mathbb{C}$, $\mathbb{N}$ 等いわゆる白抜き文字で表記する．また，零ベクトルは $\mathfrak{o}$，ゼロ行列は O と表記する．講義プリント等ではベクトルは $\boldsymbol{a}$, $\mathbf{a}$, $\mathbf{0}$, 集合では $\mathbf{R}$ と表記されていることもあったが同じ意味である．

内容に不備や落丁等がありましたら　<s17m066nk@ous.jp> へ連絡をお願いします．



目次

第 I 部
整数の性質

1　約数と倍数

1.1　整数と自然数

次の数を**整数**という.

$$\cdots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \cdots$$

整数全体の集合を $\mathbb{Z}$ とかく. また，正の整数を**自然数**という.[1] 自然数全体をなす集合を N とかく.

1.2　約数と倍数

定義

2 つの整数 $a, b\,(b \neq 0)$ について，
ある整数 k を用いて

$$a = bk$$

と表せるとき，b は a の**約数**であるといい，a は b の倍数であるという. このことを記号で，$b \mid a$ とかく.

例 1

(1) 6 の約数は $\pm1, \pm2, \pm3, \pm6$. (2) 3 の倍数は $0, \pm3, \pm6, \pm9, \pm12, \cdots$

(1)′ $\pm1 \mid 6, \pm2 \mid 6, \pm3 \mid 6, \pm6 \mid 6$. (2)′ $3 \mid 0, 3 \mid \pm3, 3 \mid \pm6, 3 \mid \pm9, 3 \mid \pm12, \ldots$

例 2

$a, b \in \mathbb{Z}$ に対して，a, b が 3 の倍数ならば，$2a + b$ も 3 の倍数である.

証明：

仮定より a, b はある整数 k, ℓ を用いて，$a = 3k$, $b = 3\ell$ と表せる. $2a + b = 2(3k) + 3\ell = 6k + 3\ell = 3(2k + \ell)$. よって $2a + b$ は 3 の倍数である. ■

1.3　素数

定義

(1) 2 以上の整数で，正の約数が 1 とその数自身のみである数を**素数**という. 2 以上の整数で，素数でない数のことを**合成数**という.

(2) 整数がいくつかの整数の積で表されるとき，そのそれぞれの整数をもとの数の**因数**という. 素数である因数のことを**素因数**という.
自然数を素数だけの積で表すことを**素因数分解する**という.

例 3

(1) 20 以下の素数：2, 3, 5, 7, 11, 13, 17, 19.
20 以下の合成数：4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20.

(2) 504 を素因数分解すると，$504 = 2^3 \cdot 3^2 \cdot 7$.

1.4　公約数と公倍数

定義

(1) $d \mid a_1, d \mid a_2, \ldots, d \mid a_n$ のとき，d は $a_1, a_2, \ldots, a_n$ の**公約数**であるという.
公約数のうち最大のものを**最大公約数**といい，$(a_1, a_2, \ldots, a_n)$ で表す.[2] $(a, b) = 1$ のとき，a, b は**互いに素**であるという.

(2) $a_1 \mid \ell, a_2 \mid \ell, \ldots, a_n \mid \ell$ のとき，ℓ は $a_1, a_2, \ldots, a_n$ の**公倍数**であるという.
公倍数のうち最小の自然数を**最小公倍数**といい，$[a_1, a_2, \ldots, a_n]$ で表す.[3]

例 4

(1) 24 と 90 の最大公約数と最小公倍数を求める.

$$\begin{array}{rrr} 2 &) & 24 \quad 90 \\ \hline 3 &) & 12 \quad 45 \\ \hline & & 4 \quad 15 \end{array}$$

$\therefore (24, 90) = 2 \cdot 3 = 6, [24, 90] = 2 \cdot 3 \cdot 4 \cdot 15 = 360.$

(2) 12, 50, 90 の最大公約数と最小公倍数を求める.

$12 = 2^2 \cdot 3, 50 = 2 \cdot 5^2, 90 = 2 \cdot 3^2 \cdot 5.$

$\therefore (12, 50, 90) = 2, [12, 50, 90] = 2^2 \cdot 3^2 \cdot 5^2 = 900.$

---

[1] 自然数に 0 を含むという流儀もあるが，ここでは含まないことにする.
[2] $\gcd(a_1, a_2, \ldots, a_n)$ と表すこともある (というかこっちの方が一般的?).
[3] $\mathrm{lcm}(a_1, a_2, \ldots, a_n)$ と表すこともある.

定理 1

$a, b \in \mathbb{Z}_{>0}$(a, b を正の整数) とし，$d = (a, b)$ とおく (a, b の最大公約数を d とおく)．このとき，次が成り立つ．
(1) ある整数 a', b' を用いて，$a = a'd, b = b'd$ と表すとき，$(a', b') = 1$.
(2) $(a, b)[a, b] = ab$.

証明：
(1) $(a', b') > 1$ と仮定すると，ある整数 a'', b'', d' を用いて，$a' = a''d', b' = b''d', d' > 1$ と表せる．
このとき，$a = a'd = a''d'd, b = b'd = b''d'd$ と表せるので，$d'd$ は a, b の公約数で，$d' > 1$ より $d'd > d$．よって矛盾．
したがって，$(a', b') = 1$.
(2) $\ell = [a, b]$ とおくと，$a \mid \ell, b \mid \ell$ (ℓ は a, b の倍数)．よって $a' \left| \frac{\ell}{d} \right., b' \left| \frac{\ell}{d} \right.$ と表せる．
ここで (1) より a', b' は互いに素であるから，$a'b' \left| \frac{\ell}{d} \right.$．つまり，$a'b'd \mid \ell$.
よって $a'b'd$ は a と b の公倍数であるから，$\ell = a'b'd = \frac{a}{d} \cdot \frac{b}{d} \cdot d$．両辺に d をかけると $d\ell = ab$. ■

2　ユークリッドの互除法

2.1　除法の定理

定理 1 (除法の定理)

整数 a と正の整数 b について，

$$a = qb + r \qquad (0 \leqslant r < b)$$

を満たす整数 q, r は 1 通りに決まる．

証明：
$\frac{a}{b}$ 以下の最大整数を q とすると，$0 \leqslant \frac{a}{b} - q < 1$．$r = a - qb$ とおくと，$a = qb + r$ であり，$0 \leqslant r < b$ を満たす.(存在性を示せた.)
次に，整数 q, q', r, r' が

$$a = qb + r = q'b + r' \qquad (0 \leqslant r \leqslant r' < b)$$

を満たすと仮定する．仮定より，$0 \leqslant r' - r < b$ かつ $r' - r = (q - q')b$ が成り立つから，$0 \leqslant q - q' < 1$.
さらに q, q' は整数より $q = q'$ である．このことから，$r' - r = (q - q')b = 0 \Leftrightarrow r' = r$ となる．したがって 1 通りである． ■

このとき，$a = qb + r$ の q を a を b で割ったときの**商**，r を a を b で割ったときの**余り**という．

例題

(1) 50 を 4 で割ったときの商と余りを求めよ．
$50 = 12 \cdot 4 + 2$．よって商は 12，余りは 2.

(2) -5 を 3 で割ったときの商と余りを求めよ．
$-5 = (-2) \cdot 3 + 1$．よって商は -2，余りは 1.[4)]

定理 2

整数 a, b, q, r ($b \neq 0$) について，

$$a = qb + r \Longrightarrow (a, b) = (b, r)$$

証明：
$d = (a, b), d' = (b, r)$ とする (a と b の最大公約数を d, b と r の最大公約数を d' とする).
a, b は d の倍数でありかつ $r = a - qb$ より，r は d の倍数である.[5)] よって d は b と r の公約数となるので $d \leqslant d'$． …❶
同様に，b, r は d' の倍数でありかつ $a = qb + r$ より，a は d' の倍数である．よって d' は a と b の公約数となるので $d' \leqslant d$． …❷
したがって ❶❷ より $d = d'$. ■

[4)] 余りが 0 以上であることに注意.
[5)] $\because$ a, b が d の倍数であるから，ある整数 k, ℓ を用いて $a = dk, b = d\ell$ と表せ，$r = a - qb = dk - q(d\ell) = d(k - q\ell)$ となる.

2.2　ユークリッドの互除法

ユークリッドの互除法

正の整数 a, b に除法の定理 (*2.1*) を順次用いると，

$$\begin{aligned}
a &= qb + r, & 0 < r < b \\
b &= q_1 r + r_1, & 0 < r_1 < r \\
r &= q_2 r_1 + r_2, & 0 < r_2 < r_1 \\
&\vdots & \vdots \\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1}, & 0 < r_{n-1} < r_{n-2} \\
r_{n-2} &= q_n r_{n-1} + r_n, & 0 < r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n + 0, & 0 = r_{n+1}
\end{aligned}$$

を満たす整数 q, q_1, q_2, …, q_{n-1}, q_n, q_{n+1}, r, r_1, r_2, …, r_{n-1}, r_n, r_{n+1} がある．定理 2 (*2.1*) より，

$$(a, b) = (b, r) = (r, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n) = r_n.$$

このようにして，a と b の最大公約数 (a, b) を求める方法を<u>ユークリッドの互除法 (Euclidean Algorithm)</u>という．

例 1

54321 と 9876 の最大公約数を求めよ．

$$\begin{aligned}
54321 &= 5 \cdot 9876 + 4941 \\
9876 &= 1 \cdot 4941 + 4935 \\
4941 &= 1 \cdot 4935 + 6 \\
4935 &= 822 \cdot 6 + 3 \\
6 &= 2 \cdot 3 + 0
\end{aligned}$$

よって 54321 と 9876 の最大公約数 $(54321, 9876) = 3$.

例 2

n を自然数とする．$n^2 + 3n + 5$ と $n + 4$ の最大公約数として考えられるものをすべて求めよ．

$$\begin{array}{rr|l}
 & n & -1 \\
\hline
n+4 & n^2 + 3n + 5 & \\
 & n^2 + 4n & \\
\hline
 & -n + 5 & \\
 & -n - 4 & \\
\hline
 & 9 &
\end{array}$$

なので，$\begin{aligned} n^2 + 3n + 5 &= (n-1) \cdot (n+4) + 9 \\ n + 4 &= \star \cdot 9 + r \quad (0 \leqslant r < 9) \end{aligned}$ とかける．

$r = 0, 1, 2, \ldots, 8$ をそれぞれ考え，ユークリッドの互除法を用いる．つまり，$(9, r)$ を考える．
$r = 0 \Rightarrow (n^2 + 3n + 5, n + 4) = 9$, $r = 1, 2, 4, 5, 7, 8 \Rightarrow (n^2 + 3n + 5, n + 4) = 1$, $r = 3, 6 \Rightarrow (n^2 + 3n + 5, n + 4) = 3$.
となるから，答えは 1, 3, 9.

突然ですが，ここで問題です．

問題 $78x + 57y = 6$ となるような整数 x, y が存在すれば 1 組求めよ．

このような問題が与えられたとき，皆さんはどのようにして x, y を見つけますか？ 恐らく，天才か解法を知っている人でなければ，地道に x の値を固定して y に一つ一つ整数を代入していくのではないだろうか？ 整数は ＋ も － もあり，そんなことをしていると日が暮れてしまう．いや日が暮れるどころか朝日が昇ってそのまた日が暮れているかもしれない．存在しない場合に限ってはこんなことをしている間に人生が終わってしまう．まぁ冗談はこのくらいにしておいて，本題へ入ろう．勘のいい人 (というか恐らくすべての人) はもう気付いているかもしれないが，これを解くのに利用するのが，ユークリッドの互除法である．詳しくは次のページで説明する．

2.3　ユークリッドの互除法の応用

前ページのユークリッドの互除法は次のように書き直すことができる．ただし r_n は最大公約数である．

$$\begin{aligned} r_n &= r_{n-2}+(-q_n)r_{n-1},\\ r_{n-1} &= r_{n-3}+(-q_{n-1})r_{n-2},\\ &\vdots\\ r_2 &= r+(-q_2)r_1,\\ r_1 &= b+(-q_1)r,\\ r &= a+(-q)b \end{aligned}$$

ここで，

$d=r_n$,

$s_1=r_{n-1}$, $s_2=r_{n-2}$, $\cdots$, $s_{n-2}=r_2$, $s_{n-1}=r_1$, $s_n=r$, $s_{n+1}=b$, $s_{n+2}=a$,　$k_1=q_n$, $k_2=q_{n-1}$, $\cdots$, $k_n=q_1$, $k_{n+1}=q$ とおいて書き直すと，

$$\begin{aligned} d &= s_2+(-k_1)s_1, && \cdots\cdots[1]\\ s_1 &= s_3+(-k_2)s_2, && \cdots\cdots[2]\\ &\vdots\\ s_{j-1} &= s_{j+1}+(-k_j)s_j, && \cdots\cdots[j]\\ &\vdots\\ s_{n-2} &= s_n+(-k_{n-1})s_{n-1}, && \cdots\cdots[n-1]\\ s_{n-1} &= s_{n+1}+(-k_n)s_n, && \cdots\cdots[n]\\ s_n &= s_{n+2}+(-k_{n+1})s_{n+1} && \cdots\cdots[n+1] \end{aligned}$$

となる．[2] の式を [1] の式に代入すると $d=s_2+(-k_1)s_1=s_2\cdot 1+(-k_1)(s_3+(-k_2)s_2)=s_3\cdot(-k_1)+s_2(1+(-k_1)(-k_2))$ となる同様に，[1] の式から [j] ($2\leqslant j\leqslant n+1$) の式までを順次代入すると，$d=s_{j+1}x_j+s_jy_j$ の形になる．ここで $x_1=1$, $y_1=-k_1$ と定める．

また，$x_2=-k_1$, $y_2=1+(-k_1)(-k_2)$, $\cdots$, $x_{j+1}=y_j$, $y_{j+1}=x_j+(-k_{j+1})y_j$ である．特に，$j=n+1$ のとき，$d=ax_{n+1}+by_{n+1}$ である．

よって次の定理を得る．

定理３

$a, b\in\mathbb{Z}$, $a, b\neq 0$ とする．d を a と b の最大公約数とする．このとき，方程式

$$ax+by=d$$

を満たす整数 x, y が存在する．

<u>証明：</u>

(i) $b>0$ の場合は，$x=x_{n+1}$, $y=y_{n+1}$ と置けば上と同じである．

(ii) $b<0$ の場合，$-b>0$ である．(i) より $-ax'-by'=d$ を満たす整数 x', y' が存在する．

$x=-x'$, $y=-y'$ と置けば，$ax+by=d$ である．　■

系１

整数 a, b が互いに素ならば，方程式

$$ax+by=1$$

を満たす整数 x, y が存在する．

例３

$78x+57y=3$ となるような整数 x, y を求める．

$$\begin{aligned} 78 &= 1\cdot 57+21\\ 57 &= 2\cdot 21+15\\ 21 &= 1\cdot 15+6\\ 15 &= 2\cdot 6+3\\ 6 &= 2\cdot 3+0 \end{aligned}$$

となるから，

	-1		-2	-1	
1	-2	3	$\boxed{-8}$	$\boxed{11}$	

より，$x=-8$, $y=11$.

2.4　ガウスの補題

定理４【ガウスの補題 (Gauss's Lemma)】

$a, b, c \in \mathbb{Z}$ とする．bc は a の倍数で，a と b が互いに素ならば，c は a の倍数である．

証明：

系１ (*2.3*) より，$ax+by=1$ を満たす整数 x, y が存在する．両辺に c をかけると，$acx+bcy=c$ である．仮定より，bc は a の倍数なので，ある整数 k を用いて，$c=acx+bcy=acx+(ak)y=a(cx+ky)$ とかける よって c は a の倍数である． ■

2.5　１次不定方程式

$a, b, c \in \mathbb{Z}(a, b \neq 0)$ とするとき，x, y の１次方程式

$$ax+by=c$$

を満たす整数 x, y の組をこの方程式の**整数解**という．また，この方程式の整数解を求めることを，**１次不定方程式を解く**という．[6]

定理５

a, b, c を整数とし，d を a, b の最大公約数とする．１次不定方程式

$$(*) \qquad ax+by=c$$

について，次が成り立つ．

(1) c が d の倍数でないとき，$(*)$ は整数解をもたない．

(2) c が d の倍数のとき，$(*)$ は整数解をもつ．$x=x_1, y=y_1$ を整数解の一つとする．このとき $a'=\dfrac{a}{d}, b'=\dfrac{b}{d}$ とおくと，$(*)$ の整数解全体は

$$x=x_1+b'k, \quad y=y_1-a'k \qquad ({}^{\forall}k \in \mathbb{Z})$$

証明：

(1) $(*)$ が整数解 x, y を持つと仮定すると，a, b は d の倍数なので $c=ax+by$ は d の倍数となる．よって矛盾．

(2) c は d の倍数なので，$\mathbb{Z} \ni c'=\dfrac{c}{d}$ とおく．ユークリッドの互除法を用いると，定理３ *(2.3)* より $ax_0+by_0=d$ を満たす整数 x_0, y_0 が存在する．両辺に c' をかけると，$a(c'x_0)+b(c'y_0)=c$．$x_1=c'x_0, y_1=c'y_0$ は，$(*)$ の整数解である：$ax_1+by_1=c$ …❶.

ここで $x=x_2, y=y_2$ を $(*)$ の任意の整数解とすると，$ax_2+by_2=c$ …❷.

❷−❶ をすると，$a(x_2-x_1)+b(y_2-y_1)=0 \Leftrightarrow a(x_2-x_1)=-b(y_2-y_1)$ …❸. 仮定より，$a=a'd, b=b'd$ なのでガウスの補題 (*2.4*) より，(x_2-x_1) は b' の倍数，つまり $x_2-x_1=b'k$ を満たす整数 k が存在する．このとき，❸ より，$y_2-y_1=-a'k$.

したがって $x_2=x_1+b'k, y_2=y_1-a'k$. ■

例３′

$78x+57y=3$ の整数解をすべて求めよ．

例３より整数解の一つは $x_1=-8, y_1=11$ である．また，$d=3$ で，$a'=\dfrac{78}{3}=26, b'=\dfrac{57}{3}=19$ となるので，$\begin{cases} x=-8+19k \\ y=11-26k \end{cases}$ $(k \in \mathbb{Z})$ である．

✍注

$(*)$ の整数解全体は

$$x=x_1-b'k, \quad y=y_1+a'k \qquad ({}^{\forall}k \in \mathbb{Z})$$

とも表される．

[6] 整数係数の方程式の整数解を求めることは，ディオファントス幾何学（**Diophantine　Geometry**）という分野につながる．

3　素数の性質

3.1　素因数分解

素数，素因数分解の定義については，*1.3* を参照.

定理 1

p を素数，$m_1, m_2, \ldots, m_k$ を整数とする．このとき，p が $m_1 m_2 \cdots m_k$ の約数ならば，p はある m_i の約数である.

証明：k についての数学的帰納法により示す.
(i) $k = 2$ のとき，p が $m_1 m_2$ の約数とする．p は素数より，p の正の約数は 1 または p なので，$(m_1, p) = 1$ または $(m_1, p) = p$ である.
$(m_1, p) = 1$ の場合，ガウスの補題 *(2.4)* より，p は m_2 の約数である．$(m_1, p) = p$ の場合，p は m_1 の約数であるので，$k = 2$ の場合は o.k.
(ii) $k > 2$ のとき，p は $m_1 \cdots m_{k-1} m_k$ の約数であるから，(i) より，p は $m_1 \cdots m_{k-1}$ または m_k の約数である.[7)]
ここで帰納法の仮定より，p が $m_1 \cdots m_{k-1}$ の約数のとき，p は $m_1, \ldots, m_{k-1}$ のいずれかの約数である．よって $k > 2$ の場合も示せた.　■

定理 2 (素因数分解)

1 より大きい整数 n は素因数分解できる．また，その分解の仕方は素数の順序を除いて 1 通りである．すなわち，同じ素数の積を 1 つの冪（べき）にまとめれば，次が成り立つ：
(1) 相異なる素数 $p_1, p_2, \ldots, p_r$ と自然数 $e_1, e_2, \ldots, e_r$ を用いて，n は

$$n = {p_1}^{e_1} {p_2}^{e_2} \cdots {p_r}^{e_r} \tag{1.1}$$

と表される.
(2) (1.1) の相異なる素数 $p_1, p_2, \ldots, p_r$ と自然数 $e_1, e_2, \ldots, e_r$ は，n に対して順序を除いて 1 通りに決まる.

証明：
n が素因数分解できることを n についての数学的帰納法で示す.
(i) $n = 2$ のとき，2 は素数なので素因数分解できた.
(ii) $n > 2$ のとき，n より小さい自然数について素因数分解できると仮定する.
n が素数ならば，n は素因数分解できた．n が合成数のとき，$n = n_1 n_2$ $(1 < n_1, n_2 < n)$ を満たす自然数 n_1, n_2 がある．帰納法の仮定より，$n_1 n_2$ は素数の積で表されるので，n も素数の積で表される.

素因数分解の仕方が順序を除いて 1 通りであることを n についての数学的帰納法で示す.
(i′) $n = 2$ のときは，明らかである.
(ii′) $n > 2$ のとき，n より小さい自然数について成り立つと仮定する．n が素数 $p, p', p'', \ldots, q, q', q'', \ldots$ を用いて

$$n = p p' p'' \cdots = q q' q'' \cdots \quad ① $$

のように 2 通りで表せたとする．定理 1 より，p は $q, q', q'', \ldots$ のいずれかの約数である.
仮に q を p の約数とすると，q は素数なので，$p = q$．①の両辺を p で割ると

$$n > p' p'' \cdots = q' q'' \cdots$$

となるので，帰納法の仮定より，$p', p'', \ldots$ と $q', q'', \ldots$ は順序を除いて等しい．よって，積に現れる素数は順序を除いて 1 通りである.　■

例 1
24 は,

$$\begin{aligned} 24 &= 2 \cdot 2 \cdot 2 \cdot 3 = 2 \cdot 2 \cdot 3 \cdot 2 = 2 \cdot 3 \cdot 2 \cdot 2 = 3 \cdot 2 \cdot 2 \cdot 2 \\ &= 2^3 \cdot 3 = 3 \cdot 2^3 \end{aligned}$$

という形に素因数分解できる.

[7)] (i) の場合の $m_1 = m_1 \cdots m_{k-1}$, $m_2 = m_k$ と考えられるから.

定理 3

正の整数 a, b の素因数分解に現れる素数を合わせて，p_1, p_2, …, p_n (これらは相異なる) とする．

$$a = {p_1}^{e_1}{p_2}^{e_2}\cdots{p_n}^{e_n},\ b = {p_1}^{f_1}{p_2}^{f_2}\cdots{p_n}^{f_n} \qquad (\mathbb{Z} \ni e_1, e_2, \ldots, e_n, f_1, f_2, \ldots, f_n \geqslant 0)$$

のとき，a, b の最大公約数 (a, b)，最小公倍数 $[a, b]$ は，

$$(a, b) = {p_1}^{\min\{e_1, f_1\}}{p_2}^{\min\{e_2, f_2\}}\cdots{p_n}^{\min\{e_n, f_n\}},\quad [a, b] = {p_1}^{\max\{e_1, f_1\}}{p_2}^{\max\{e_2, f_2\}}\cdots{p_n}^{\max\{e_n, f_n\}}$$

で与えられる．

証明：

a, b の正の公約数 d は

$$d = {p_1}^{g_1}{p_2}^{g_2}\cdots{p_n}^{g_n},\quad 0 \leqslant g_i \leqslant e_i,\quad 0 \leqslant g_i \leqslant f_i \qquad (i = 1, 2, \ldots, n)$$

と表される．(a, b) は上の条件を満たす最大の g_i $(i = 1, 2, \ldots, n)$ に対応する[8]から，$g_i = \min\{e_i, f_i\}$ $(i = 1, 2, \ldots, n)$.

$[a, b]$ については，*1.4* の定理 1 (2) より，$(a, b)[a, b] = ab$ より，$[a, b] = \dfrac{ab}{(a, b)}$ である．仮定と上記の結果から，

$$[a, b] = \frac{ab}{(a, b)} = \frac{({p_1}^{e_1}{p_2}^{e_2}\cdots{p_n}^{e_n})({p_1}^{f_1}{p_2}^{f_2}\cdots{p_n}^{f_n})}{(a, b)} = \frac{{p_1}^{e_1+f_1}{p_2}^{e_2+f_2}\cdots{p_n}^{e_n+f_n}}{{p_1}^{\min\{e_1, f_1\}}{p_2}^{\min\{e_2, f_2\}}\cdots{p_n}^{\min\{e_n, f_n\}}}$$

となる．ここで，

$$e_i + f_i = \min\{e_i, f_i\} + \max\{e_i, f_i\}$$

なので，

$$\begin{aligned}[a, b] &= \frac{{p_1}^{e_1+f_1}{p_2}^{e_2+f_2}\cdots{p_n}^{e_n+f_n}}{{p_1}^{\min\{e_1, f_1\}}{p_2}^{\min\{e_2, f_2\}}\cdots{p_n}^{\min\{e_n, f_n\}}} = {p_1}^{(e_1+f_1)-\min\{e_1, f_1\}}{p_2}^{(e_2+f_2)-\min\{e_2, f_2\}}\cdots{p_n}^{(e_n+f_n)-\min\{e_n, f_n\}} \\ &= {p_1}^{\max\{e_1, f_1\}}{p_2}^{\max\{e_2, f_2\}}\cdots{p_n}^{\max\{e_n, f_n\}}\end{aligned}$$

である． ■

3.2　エラトステネスのふるい

素数の求め方として，**エラトステネスの篩** (ふるい) (Sieve of Eratosthenes) と呼ばれる方法がある．

例えば，100 までの素数をすべて求めるとき，2 から 100 までの数をすべて書き出し，次の手順に沿って数を消していく．このとき，最後に残った数が 100 までの素数となる．最小の数は 2 である．これを残して，2 の倍数をすべて消す．2 の次に最小となる数は 3 である．これを残して，3 の倍数をすべて消す．3 の次に最小の数は 5 である．これを残して，5 の倍数をすべて消す．5 の次に最小の数は 7 である．これを残して，7 の倍数をすべて消す．新たに消すことができる数がなくなるまでこの作業を繰り返す．

➡注

n までの素数を求める場合，$\sqrt{n}$ 以下の整数の倍数まで上の作業を行えばよい.[9]

問題 エラトステネスの篩を用いて，100 以上 121 以下の素数をすべて求め，その個数を答えよ．

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61
62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81
82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101
102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121

解答 101, 103, 107, 109, 113 で，5 個．

[8] つまり，共通素因数 p_i の冪 e_i と f_i に対応するという意味である．

[9] $\sqrt{n}$ が関係したのは，n が合成数なら必ず $\sqrt{n}$ より小さい素因数があるので．

3.3　素数の無限性

定理

素数の個数は無限である.

証明：ユークリッドの証明

素数の個数が有限であると仮定する．全ての素数を p_1, p_2, ..., p_n とする．このとき，

$$q = p_1 p_2 \cdots p_n + 1$$

は 1 より大きいので，合成数か素数である．q が合成数であると仮定すると，q はある p_i の倍数となるはずだが，$p_1 p_2 \cdots p_n + 1$ を割らないので，矛盾．よって q は素数となる．しかし，q は p_1, p_2, ..., p_n と異なるので，$q \notin \{p_1, p_2, \ldots, p_n\}$ =（素数全体をなす集合）となり矛盾．したがって，素数の個数は無限である． ■

* ユークリッドの証明以外の証明方法もたくさんある．参考 ☞ **https://mathtrain.jp/prime**

3.4　双子素数

定義【双子素数】

引き続いた 2 つの奇数がともに素数のとき，それらを**双子素数**という.

例 2

3 と 5，5 と 7，11 と 13，17 と 19，29 と 31，41 と 43 は双子素数である.

未解決問題

双子素数の個数は無限か？

3.5　素数の分布

• 2 3 • 5 • 7 • • • 11 • 13 • • • 17 • 19 • • • 23 • • • • • 29 • 31 • •
• • • 37 • • • 41 • 43 • • • 47 • • • • • 53 • • • • • 59 • 61 • • • • •

定理 4

p を素数とするとき，p 以下のすべての素数の積に 1 加えた数を $q(= 2 \cdot 3 \cdot 5 \cdots p + 1)$ とおくと，p の次に大きい素数は q 以下である.

証明：

p' を q の素因数とすると，$p < p'$．$\therefore p <$ p の次に大きい素数 $\leqslant p' \leqslant q$. ■

定理 5

いくらでも大きい間隔をもつ 2 つの素数を見つけることができる.

証明：

n を任意の自然数としたとき，次の $(n-1)$ 個の連続した自然数

$$\begin{aligned} n!+2 &= 1 \cdot 2 \cdots n+2 = 2 \cdot (1 \cdot 3 \cdot 4 \cdots n+1) \\ n!+3 &= 1 \cdot 2 \cdots n+3 = 3 \cdot (1 \cdot 2 \cdot 4 \cdots n+1) \\ &\vdots \\ n!+n &= 1 \cdot 2 \cdots n+n = n \cdot (1 \cdot 2 \cdots (n-1)+1) \end{aligned}$$

はすべて合成数である. ■

3.6　$2^n \pm 1$ の形の素数 (メルセンヌ素数・フェルマー素数)

定義【メルセンヌ素数 (Mersenne prime)】

$$M_p = 2^p - 1 \quad (p \in \mathbb{N})$$

の形の数を**メルセンヌ数** (Mersenne number) という．M_p が素数のとき，M_p を**メルセンヌ素数**という．

定理 6

$M_p = 2^p - 1$ がメルセンヌ素数ならば，p は素数である．

証明：
仮定より $p > 1$．p が合成数であると仮定すると，$p = ab$ $(1 < a, b < p)$ を満たす自然数 a, b が存在する．つまり，

$$M_p = 2^p - 1 = 2^{ab} - 1 = (2^a - 1)\left\{2^{a(b-1)} + 2^{a(b-2)} + \cdots + 1\right\}$$

は 1 より大きい自然数の積となり，M_p が素数であることに矛盾する． ■

➪**注** p が素数だからといいて M_p が素数とは限らない．例えば $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$ など．

20 番目までのメルセンヌ素数 M_p は，

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423$$

によって与えられる．

未解決問題

メルセンヌ素数の個数は無限か？[10)]

定義【フェルマー素数】

$$F_n = 2^{2n} + 1 \quad (\mathbb{Z} \ni n \geqslant 0)$$

の形の数を**フェルマー数** (Fermat number) という．F_n が素数のとき，F_n を**フェルマー素数**という．

フェルマーは，F_n はすべて素数になるであろうと予想した．実際に計算すると，

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537$$

は素数だが，$F_5 = 4294969297 = 641 \cdot 6700417$ は合成数である．現在知られている最大のフェルマー素数は F_4 である．[11)]

未解決問題

フェルマー素数の個数は無限か？

問題 5 以上の素数は自然数 n を用いて $6n - 1$ または $6n + 1$ の形で表せることを示せ．

解答 5 以上の自然数は，$6n - 1,\ 6n + 1,\ 6n + 2,\ 6n + 3,\ 6n + 4$ $(n \in \mathbb{N})$ と表せる．
$6n + 2 = 2(3n + 1),\ 6n + 3 = 3(2n + 1),\ 6n + 4 = 2(3n + 2)$ と表せるので，$6n + 2,\ 6n + 3,\ 6n + 4$ は合成数である．
したがって，5 以上の素数は $6n - 1$ または $6n + 1$ の形で表せる． ■

[10)] 新しいメルセンヌ素数を見つけると 3000$，1 億桁以上のメルセンヌ素数を見つけると 50000$もらえるらしい．
[11)] フェルマー素数に関する定理で有名なのが，作図に関する定理である．正 n 角形の図形が定規とコンパスのみで作図可能 $\Leftrightarrow$ n がフェルマー素数の積でかける．

4　合同式

4.1　合同式

定義【合同式】

n を自然数，a, b を整数とする．$a-b$ が n の倍数のとき，a と b は n を法として**合同**であるといい，

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

とかく．この式のことを**合同式**という．[12)]

例 1

(1) $5-2=3=3\cdot 1$ より，$5 \equiv 2 \pmod 3$.　　(2) $4-(-5)=9=3\cdot 3$, $4-1=3=3\cdot 1$ より，$4 \equiv -5 \pmod 3 \equiv 1 \pmod 3$.

命題 1

a, b が n で割り算をして余りが等しいとき，a, b は n を法として合同である．

証明：
仮定より，ある整数 q, q', r を用いて，$a=qn+r$, $b=q'n+r$ $(0 \leqslant r < n)$ とかける．
$a-b=qn+r-(q'n+r)=(q-q')n$ となる．合同式の定義より，$a \equiv b \pmod n$　■

基本的に $* \equiv a \pmod n$ は $a=0, 1, \ldots, n-1$ で表すことが多い．

定理 1

$n \in \mathbb{N}$, $a, b, c \in \mathbb{Z}$ に対して，次が成り立つ．
(1) (反射律)　$a \equiv a \pmod n$.
(2) (対称律)　$a \equiv b \pmod n \Longrightarrow b \equiv a \pmod n$.
(3) (推移律)　$a \equiv b \pmod n$, $b \equiv c \pmod n \Longrightarrow a \equiv c \pmod n$.

証明：
(1) $a-a=0=n\cdot 0$. 合同式の定義より，$a \equiv a \pmod n$.
(2) 仮定より，$a-b=nk$ となるような整数 k がある．$b-a=-(a-b)=-nk=n\cdot(-k)$ となるので，$b \equiv a \pmod n$.
(3) 仮定より，$a-b=nk$, $b-c=n\ell$ なるような整数 k, ℓ がある．$a-c=(a-b)+(b-c)=nk+n\ell=n(k+\ell)$ となる．
よって $a \equiv c \pmod n$.　■

4.2　合同式の加減乗法

定理 2

$n \in \mathbb{N}$, $a, a', b, b' \in \mathbb{Z}$ が，$a \equiv a' \pmod n$, $b \equiv b' \pmod n$ を満たすとき，次が成り立つ．

$$\begin{aligned} a+b &\equiv a'+b' \pmod n \\ a-b &\equiv a'-b' \pmod n \\ ab &\equiv a'b' \pmod n \end{aligned}$$

証明：仮定より，$a-a'=nk$, $b-b'=n\ell$ を満たす整数 k, ℓ がある．
$(a+b)-(a'+b')=(a-a')+(b-b')=nk+n\ell=n(k+\ell)$, $(a-b)-(a'-b')=(a-a')-(b-b')=nk-n\ell=n(k-\ell)$.
$ab-a'b'=ab-a'b'+0=ab-a'b'-a'b+a'b=(a-a')b+a'(b-b')=nkb+a'n\ell=n(kb+a'\ell)$.
したがって，成り立つ．　■

[12)] ≡ はガウスが生み出した記号である．数学の整数論を大きく発展させた．

定理 2 (*4.2*) より，次のことがわかる．

系 1

自然数 n と整数 a, b が，$a \equiv b \pmod{n}$ を満たすならば，任意の自然数 m について，

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

が成り立つ．

例 2

(1) 2^{100} を 7 で割った余りを求める．

2^{100} を mod 7 で考える．$2^{100} = (2^3)^{33} \cdot 2 = 8^{33} \cdot 2 \equiv 1^{33} \cdot 2 \pmod{7} \equiv 1 \cdot 2 \equiv 2 \pmod{7}$．よって余りは 3.

(2) 23^{23} の一の位の数を求める．

23^{23} を mod 10 で考える．

$23 \equiv 3 \pmod{10}$, $3^2 = 9 \equiv -1 \pmod{10}$ であることを用いると，

$23^{23} = (23^2)^{11} \cdot 23 \equiv (3^2)^{11} \cdot 3 \equiv (-1)^{11} \cdot 3 = -3 \equiv 7 \pmod{10}$．よって一の位の数は 7.

4.3　合同式の除法

定理 3

自然数 n と整数 a, b, c に対して，次が成り立つ．

(1) $(c, n) = 1$ のとき，$ac \equiv bc \pmod{n} \Longrightarrow a \equiv b \pmod{n}$.

(2) $(c, n) = d > 1$ のとき，$ac \equiv bc \pmod{n} \Longrightarrow a \equiv b \pmod{\frac{n}{d}}$.

証明：

(1) 仮定より $ac - bc = (a-b)c$ は n の倍数である．いま，$(c, n) = 1$ なので，ガウスの補題 (*2.4*) より $a - b$ は n の倍数である．

(2) $n' = \frac{n}{d}$, $c' = \frac{c}{d}$ とおくと，$(n', c') = 1$．$ac - bc = (a-b)c = (a-b)c'd$ は $n(= n'd)$ の倍数なので，$(a-b)c'$ は n' の倍数である．$(c', n') = 1$ なので，ガウスの補題より，$a - b$ は n' の倍数である．　■

例 3

(1) $\underbrace{40}_{=8\cdot5} \equiv \underbrace{10}_{=2\cdot5} \pmod{6}$ は $(5, 6) = 1$ なので，両辺を 5 で割ると，$8 \equiv 2 \pmod{6}$.

(2) $\underbrace{28}_{=7\cdot4} \equiv \underbrace{16}_{=4\cdot4} \pmod{6}$ は $(4, 6) = 2$, $\frac{6}{2} = 3$ なので両辺を 4 で割ると，$7 \equiv 4 \pmod{3}$.

4.4　合同式を解く

合同式を満たす x をすべて求めることを，合同式を**解く**という．

例 4

(1) $3x \equiv 5 \pmod{7}$ を解く．

$(3, 7) = 1$ なので，両辺に 5 をかけると，$15x \equiv 25 \pmod{7}$．$15 \equiv 1 \pmod{7}$ より，$15x \equiv x \equiv 25 \equiv 4 \pmod{7}$．　$\therefore x \equiv 4 \pmod{7}$.

(2) $7x \equiv 3 \pmod{15}$ を解く．

$(7, 15) = 1$ より，両辺を -2 倍すると，$-14x \equiv -6 \pmod{15}$.

$-14 - 1 = -15 = 15 \cdot (-1)$ より，$-14 \equiv 1 \pmod{15}$，また $-6 - 9 = -15$ より，$-6 \equiv 9 \pmod{15}$ なので，$x \equiv 9 \pmod{5}$.

……

演習 次の合同式を解け．

(1) $4x \equiv 2 \pmod{5}$

(2) $5x \equiv 8 \pmod{13}$

(3) $8x \equiv 1 \pmod{13}$

解

(1) $x \equiv 3 \pmod{5}$

(2) $x \equiv 12 \pmod{13}$

(3) $x \equiv 5 \pmod{13}$

4.5　倍数の判定法 (10 進法)

自然数 N が，10 進法で

$$N = a_n \cdots a_2 a_1 \qquad (0 \leqslant a_1,\, a_2,\, \ldots,\, a_n < 10,\, a_n \neq 0)$$

と表せる[13]とすると，

$$N = a_n \times 10^{n-1} + \cdots + a_2 \times 10 + a_1.$$

このとき，桁に現れる数の和を $S(N)$ とおく：

$$S(N) = a_n + \cdots + a_2 + a_1.$$

定理４【倍数の判定法 (その１)】

10 進法の自然数 $N = a_n \cdots a_2 a_1$ について，次が成り立つ．

(1) a_1 が 2 の倍数ならば，N は偶数である．　(2) $S(N)$ が 3 の倍数ならば，N は 3 の倍数である．

(3) a_1 が 5 の倍数ならば，N は 5 の倍数である．　(4) $S(N)$ が 9 の倍数ならば，N は 9 の倍数である．

証明：

(1) 仮定より，$a_1 \equiv 0 \pmod 2$．また，$10 \equiv 0 \pmod 2$ より $N \equiv a_n \times 0^{n-1} + \cdots + a_2 \times 0 + a_1 = a_1 \equiv 0 \pmod 2$．

(2) 仮定より，$a_n + \cdots + a_2 + a_1 \equiv 0 \pmod 3$．また，$10 \equiv 1 \pmod 3$ より，
$N \equiv a_n \times 1^{n-1} + \cdots a_2 \times 1 + a_1 = a_n + \cdots + a_2 + a_1 \equiv 0 \pmod 3$．

(3) 仮定より，$a_1 \equiv 0 \pmod 5$．また，$10 \equiv 0 \pmod 5$ より，$N \equiv a_n \times 0^{n-1} + \cdots + a_2 \times 0 + a_1 = a_1 \equiv 0 \pmod 5$．

(4) 仮定より $a_n + \cdots + a_2 + a_1 \equiv 0 \pmod 9$．また，$10 \equiv 1 \pmod 9$ より，
$N \equiv a_n \times 1^{n-1} + \cdots a_2 \times 1 + a_1 = a_n + \cdots + a_2 + a_1 \equiv 0 \pmod 9$．　■

定理５【倍数の判定法 (その２)】

10 進法の自然数 $N = a_n \cdots a_2 a_1$ について，次が成り立つ．

(1) 下 2 桁の数 $a_2 a_1$ が 4 の倍数ならば，N は 4 の倍数である．

(2) a_1 が 2 の倍数で，$S(N)$ が 3 の倍数ならば，N は 6 の倍数である．

(3) N を下から 3 桁ずつ区切っていく．このとき，$a_3 a_2 a_1 - a_6 a_5 a_4 + a_9 a_8 a_7 - \cdots$ が 7 の倍数ならば，N は 7 の倍数である．

(4) 下 3 桁の数 $a_3 a_2 a_1$ が 8 の倍数ならば，N は 8 の倍数である．

(5) $a_1 - a_2 + a_3 - \cdots + (-1)^{n-1} a_n$ が 11 の倍数ならば，N は 11 の倍数である．

証明：

(1) 仮定より，$a_2 \times 10 + a_1 \equiv 0 \pmod 4$．また，$10 \equiv 2 \pmod 4$, $10^2 \equiv 0 \pmod 4$ より，$10^k \equiv 0 \pmod 4$ $(\mathbb{N} \ni {}^\forall k \geqslant 2)$ なので，
$N \equiv a_n \times 0^{n-1} + \cdots + a_3 \times 0^2 + a_2 \times 10 + a_1 \equiv a_2 \times 10 + a_1 \equiv 0 \pmod 4$．

(2) 定理 4 の (1),(2) より．

(3) 仮定より，$a_3 a_2 a_1 - a_6 a_5 a_4 + a_9 a_8 a_7 - \cdots \equiv 0 \pmod 7$．
また，$10 \equiv 3 \pmod 7$ より $10^3 \equiv 27 \equiv -1 \pmod 7$, $10^6 \equiv -1 \pmod 7$, $10^9 \equiv -1 \pmod 7$, $\cdots$．このとき，
$N \equiv a_3 a_2 a_1 + a_6 a_5 a_4 \times 10^3 + a_9 a_8 a_7 \times 10^6 + \cdots \pmod 7 \equiv a_3 a_2 a_1 - a_6 a_5 a_4 + a_9 a_8 a_7 - \cdots \equiv 0 \pmod 7$．

(4) 仮定より，$a_3 \times 10^3 + a_2 \times 10 + a_1 \equiv 0 \pmod 8$．
また，$10^3 = (2 \cdot 5)^3 = 2^3 \cdot 5^3 = 8 \cdot 5 \equiv 0 \cdot 5 \pmod 8 \equiv 0 \pmod 8$ より，$10^\ell \equiv 0 \pmod 8$ $(\mathbb{N} \ni {}^\forall \ell \geqslant 3)$ なので，
$N \equiv a_n \times 0^{n-1} + \cdots + a_4 \times 0^3 + a_3 \times 10^2 + a_2 \times 10 + a_1 = a_3 \times 10^2 + a_2 \times 10 + a_1 \equiv 0 \pmod 8$．

(5) 仮定より，$a_n \times (-1)^{n-1} + \cdots + a_2 \times (-1) + a_1 \equiv 0 \pmod{11}$．また，$10 \equiv -1 \pmod{11}$ より，$10^m \equiv (-1)^m \pmod{11}$ $({}^\forall m \in \mathbb{N})$．
よって，$N \equiv a_n \times (-1)^{n-1} + \cdots + a_2 \times (-1) + a_1 \equiv 0 \pmod{11}$．　■

例５

(1) 32910423 は 7 の倍数である．

(2) 47654321 は 11 の倍数である．

[13] $N = a_n \cdots a_2 a_1$ は乗法ではなく数を並べたもである，例えば，$N = 1 \cdot 2 = 2$ ではなく，$N = 12$.

4.6　1 次合同式

n を自然数，a, b は整数とする．このとき，$a \not\equiv 0 \pmod{n}$ を仮定して，1 次合同式

(∗)　　$$ax \equiv b \pmod{n}$$

を解きたい．

(∗) が解を持つ $\Longleftrightarrow$ $ax-b$ が n の倍数となるような整数 x が存在 $\Longleftrightarrow$ $ax-b=ny$ を満たすような整数 x, y が存在，つまり，

(∗∗)　　$ax \equiv b \pmod{n}$ が解をもつ $\Longleftrightarrow$ $ax+ny=b$ を満たす整数 x, y がある

となる．ゆえに，次がわかる．

定理 6

n を自然数，a, b を整数とし，d は a, n の最大公約数とする．さらに，$a \not\equiv 0 \pmod{n}$ とする．このとき，1 次合同式

(∗)　　$$ax \equiv b \pmod{n}$$

について，次が成り立つ．

(1) b が d の倍数でないとき，(∗) は解をもたない．

(2) b が d の倍数のとき，(∗) は解をもつ．$x=x_1$ を (∗) の解の 1 つとする．$n'=\dfrac{n}{d}$ とおくと，(∗) の解全体は

$$x = x_1 + n'k \quad (^{\forall}k \in \mathbb{Z})$$

である．これを合同式で表すと，(∗) の解は

$$x \equiv x_1,\ x_1+n',\ \cdots,\ x_1+(d-1)n' \pmod{n}.$$

証明：

(1) (∗∗) と *2.5* の定理 5 よりわかる．

(2) (∗∗) と *2.5* の定理 5 よりわかる．また，(∗) の解全体は $x=x_1+n'k$ $(k \in \mathbb{Z})$.

これらの解を法を n として区別する．k, k' を整数とするとき，

$$x_1+n'k \equiv x_1+n'k' \pmod{n} \iff n'k \equiv n'k' \pmod{\underbrace{n}_{=n'd}} \iff k \equiv k' \pmod{d}$$

となるので，d を法としての k の取り方は d 通りである．[14] よって，n を法として互いに合同でない解は全部で d 個ある．　■

定理 7

n は自然数で，a は n と互いに素な整数とすると

$$ac \equiv 1 \pmod{n}$$

を満たす整数 c が n を法としてただ 1 つある．

証明：

a, n の最大公約数は 1 なので，定理 6 より，$ax \equiv 1 \pmod{n}$ は解をもつ．

c をこの合同式の解の 1 つとすると，解は $d=1$ 個あるので，$x \equiv c \pmod{n}$.　■

演習 次の 1 次合同式を解け．

(1) $8x \equiv 6 \pmod{14}$　　ヒント：$ax+ny=b$ の形にして解く．

(2) $66x \equiv 100 \pmod{121}$

解

(1) $x=6+7k$ $(k \in \mathbb{Z})$ または $x \equiv 6 \pmod{14}$, $x \equiv 6+7 \equiv 13 \pmod{14}$.

(2) 解なし．

[14] d で割った余りは $0, 1, \ldots, d-1$ なので d 個．

4.7　連立 1 次合同式

いくつかの 1 次合同式

$$\begin{cases} b_1x \equiv a_1 \pmod{n_1} \\ b_2x \equiv a_2 \pmod{n_2} \\ \qquad\vdots \\ b_kx \equiv a_k \pmod{n_k} \end{cases}$$

を満たす解 x を求めることを連立 1 次合同式を**解く**という.

4.7.1　補助定理

補題 1

自然数 $n_1, n_2, \ldots, n_k$ はどの 2 つも互いに素であるとする．このとき，整数 a が $n_1, n_1, \ldots, n_k$ の倍数ならば，a は積 $n_1n_2\cdots n_k$ の倍数である.

証明：k に関する数学的帰納法により示す.

(i) $k = 2$ のとき，$a = mn_1$ を満たす整数 m がある.

a は n_2 の倍数で，n_1 と n_2 は互いに素であるから，ガウスの補題 (*2.4*) より，m は n_2 の倍数なので，a は n_1n_2 の倍数である.

(ii) $k > 2$ の場合において，$k - 1$ のとき主張が成り立つと仮定する.

$\ell = n_1n_2\cdots n_{k-1}$ とおくと，帰納法の仮定より，a は ℓ の倍数である．ℓ と n_k は互いに素であるから，

$k = 2$ の場合により，a は $\ell n_k = n_1n_2\cdots n_{k-1}n_k$ の倍数である. ■

4.7.2　中国式剰余定理

定理【中国式剰余定理】(Chinese remainder theorem)

自然数 $n_1, n_2, \ldots, n_k$ はどの 2 つも互いに素であるとする．$a_1, a_2, \ldots, a_k$ を整数とするとき，連立 1 次合同式

$$(*) \qquad \begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \qquad\vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

を満たす解は，積 $N = n_1n_2\cdots n_k$ を法としてただ 1 つある．つまり，$x = x_0$ が (∗) の解の 1 つならば，(∗) の解全体は

$$x = x_0 + N\ell \quad (\ell \in \mathbb{N})$$

これを合同式で表すと

$$x \equiv x_0 \pmod{N}.$$

証明：ガウスの証明

(解の存在を示す)

$N_1 = \dfrac{N}{n_1}, N_2 = \dfrac{N}{n_2}, \ldots, N_k = \dfrac{N}{n_k}$ とおくと，

$$N = n_1N_1 = n_2N_2 = \cdots = n_kN_k, \quad (n_1, N_1) = (n_2, N_2) = \cdots = (n_k, N_k) = 1.$$

定理 7 (*4.6*) より，各 i $(1 \leqslant i \leqslant k)$ について，

$$N_it_i \equiv 1 \pmod{n_i}$$

を満たす整数 t_i が n_i を法としてただ 1 つある.

$$x_0 = a_1N_1t_1 + a_2N_2t_2 + \cdots + a_kN_kt_k$$

は，(∗) の解である.[15] よって，$x_0 \equiv a_iN_it_i + \sum_{j \neq i} a_jN_jt_j \equiv a_i + \sum_{j \neq 0} a_j0t_j \equiv a_i \pmod{n_i}$.

(唯一性を示す)

x_1 を (∗) の解とすると，各 i $(1 \leqslant i \leqslant k)$ について，$x_1 \equiv a_i \equiv x_0 \pmod{n_i}$ なので，$x_1 - x_0$ は，$n_1, n_2, \ldots, n_k$ の倍数である.

補題 1 より，$x_1 - x_0$ は $n_1, n_2, \ldots, n_k = N$ の倍数となり，$x_1 \equiv x_0 \pmod{N}$. ■

[15] 各 i $(1 \leqslant i \leqslant k)$ について，N_j $(j \neq i)$ は n_i の倍数なので.
例えば，$x_0 \equiv a_1 \underbrace{N_it_1}_{\equiv 1} + a_2 \underbrace{N_2}_{\equiv 0} t_2 + \cdots + a_k \underbrace{N_k}_{\equiv 0} t_k \equiv a_1 \pmod{n_1}$.

4.8　連立 1 次合同式 例題

例題

(1) (ガウス式)

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}, \quad \begin{matrix} n_1 = 3 \\ n_2 = 5, \\ n_3 = 7 \end{matrix} \quad N = 3\cdot 5\cdot 7 = 105, \quad \begin{matrix} N_1 = 35(=\frac{N}{n_1}), & 35t_1 \equiv 1 \pmod 3 \equiv 2t_1, & t_1 = 2. \\ N_2 = 21(=\frac{N}{n_2}), & 21t_2 \equiv 1 \pmod 5 \equiv t_2, & t_2 = 1. \\ N_3 = 15(=\frac{N}{n_3}), & 15t_3 \equiv 1 \pmod 7 \equiv t_3, & t_3 = 1. \end{matrix}$$

$x_0 = a_1N_1t_1 + a_2N_2t_2 + a_3N_3t_3 = 2\cdot 35\cdot 2 + 3\cdot 21\cdot 1 + 2\cdot 15\cdot 1 = 233.$ $\therefore x = 233 + 105k$ $(k \in \mathbb{Z})$ または $x \equiv 233 \equiv 23 \pmod{105}$.

(2) (中国式)

$$\begin{cases} x \equiv 1 \pmod 7 & \cdots ❶ \\ x \equiv 2 \pmod{11} & \cdots ❷ \end{cases}$$

❶ より $x = 7k + 1$　$k \in \mathbb{Z}$ とかける．これを ❷ に代入する．$7k + 1 \equiv 2 \pmod{11} \Leftrightarrow 7k \equiv 1 \pmod{11}$．$k = 8$ とすればよい．

$k = 8$ は解なので，$x = 7k + 1 = 7\cdot 8 + 1 = 57$ は $\begin{cases} x \equiv 1 \pmod 7 \\ x \equiv 2 \pmod{11} \end{cases}$ の解である．よって $x \equiv 57 \pmod{77}$.

4.9　２項展開

定理８

p を素数，a, b を整数とするとき，

$$(a+b)^p \equiv a^p + b^p \pmod p.$$

証明：

２項定理より，

$$(a+b)^p = \sum_{r=0}^{p} \binom{p}{r} a^r b^{p-r}.$$

$0 < r < p$ のとき，$\binom{p}{r} = \dfrac{p!}{r!(p-r)!} \Leftrightarrow p! = \binom{p}{r} r!(p-r)!$ の右辺は明らかに p の倍数であり，$r!(p-r)!$ は p の倍数でない[16]ので，ガウスの補題 (*2.4*) より，$\binom{p}{r}$ は p の倍数である．よって，

$$(a+b)^p = a^p + \underbrace{\sum_{r=1}^{p-1} \binom{p}{r} a^r b^{p-r}}_{\equiv 0} + b^p \equiv a^p + b^p \pmod p. \qquad \blacksquare$$

[16] p は素数なので．

4.10　フェルマーの小定理

フェルマーの小定理 (**Fermat's little theorem**)

p を素数，a を整数とするとき，

(*)　$$a^p \equiv a \pmod{p}.$$

さらに a と p が互いに素ならば，両辺を a で割って，

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

証明：

(I) $a > 0$ の場合：a についての数学的帰納法により示す.

(i) $a = 1$ のとき，明らかに $1^p \equiv 1 \pmod{p}$ なので成り立つ.

(ii) a のとき，$a^p \equiv a \pmod{p}$ が成り立つと仮定する.

$a+1$ のとき，*4.9* の定理 8 より，$(a+1)^p \equiv a^p + 1^p \pmod{p}$.

また，帰納法の仮定より，$a^p + 1^p \equiv a + 1 \pmod{p}$．$\therefore (a+1)^p \equiv a + 1 \pmod{p}$．よって $a+1$ のときも成り立つ.

(II) $a = 0$ の場合，明らかに $0^p \equiv 0 \pmod{p}$ なので成り立つ.

(III) $a < 0$ の場合，$-a > 0$ なので (I) より，

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

両辺に $-1 \pmod{p}$ をかけると，$a^p \equiv a \pmod{p}$.　■

フェルマーの小定理の対偶

互いに素な正の整数 a, n が

$$a^{n-1} \not\equiv 1 \pmod{n}$$

を満たすとき，n は素数ではない.

この素数判定法を**フェルマーテスト**という.

⇨注 合成数 n で，互いに素な整数 a について，

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

を満たすものがある．このような n を**擬素数**という.

例 6 (フェルマーテスト)

$2^{n-1} \not\equiv 1 \pmod{n}$ を満たす奇数 n は素数ではない.

例 7 (擬素数)

$341 = 11 \cdot 31$ であるが，$2^{341-1} = 2^{340} = (2^{10})^{34} = 1024^{34} = (3 \cdot 341 + 1)^{34} \equiv 1 \pmod{341}$．341 は 2 に対する擬素数である.

例題

(1) 29^{1000} を 13 で割った余りを求めよ.

$(29, 13) = 1$ より，フェルマーの小定理より $29^{13-1} = 29^{12} \equiv 1 \pmod{13}$.

また，$29 \equiv 3 \pmod{13}$ なので，$29^{1000} = (29^{12})^8 \cdot 29^4 \equiv 1^8 \cdot 3^4 = 81 \equiv 3 \pmod{13}$．よって余りは 3.

(2) $x^{107} \equiv 3 \pmod{5}$

$x \equiv 0 \not\equiv 3 \pmod{5}$ より $x \not\equiv 0 \pmod{5}$ なので，$(x, 5) = 1$．フェルマーの小定理より，$x^{5-1} = x^4 \equiv 1 \pmod{5}$.

$x^{107} = (x^4)^{26} \cdot x^3 \equiv x^3 \equiv 3 \pmod{5}$ に $x = 1, 2, 3, 4$ を代入して確かめると，

$x = 1 \Rightarrow 1 \not\equiv 3$, $x = 2 \Rightarrow 2^3 = 8 \equiv 3 \pmod{5}$ なので o.k. $x = 3 \Rightarrow 3^3 = 27 \equiv 2 \not\equiv 3$, $x = 4 \Rightarrow 4^3 = 256 \equiv 1 \not\equiv 3$．よって $x \equiv 2 \pmod{5}$.

5　RSA 暗号

5.1　オイラー関数

定義【オイラー関数 (Euler's totient function)】

n を自然数とする．1, 2, …, n の中で n と互いに素となる自然数の個数を $\varphi(n)$ で表す．この φ を**オイラー関数**という．

n	1, 2, …, n の中で n と互いに素な自然数	$\varphi(n)$
1	1	1
2	1	1
3	1, 2	2
4	1, 3	2
5	1, 2, 3, 4	4
6	1, 5	2
7	1, 2, 3, 4, 5, 6	6
8	1, 3, 5, 7	4
9	1, 2, 4, 5, 7, 8	6
10	1, 3, 7, 9	4

定理 1

(1) 素数 p と自然数 k に対して，$\varphi(p^k) = p^k - p^{k-1}$.

(2) m, n を互いに素な自然数とするとき，$\varphi(mn) = \varphi(m)\varphi(n)$.

(3) 自然数 n の素因数分解を $n = {p_1}^{e_1}{p_2}^{e_2}\cdots{p_r}^{e_r}$ とするとき，

$$\varphi(n) = ({p_1}^{e_1} - {p_1}^{e_1-1})({p_2}^{e_2} - {p_2}^{e_2-1})\cdots({p_r}^{e_r} - {p_r}^{e_r-1}).$$

証明：

(1) a を $1 \leqslant a \leqslant p^k$ を満たす自然数とする．$(a,\ p) \neq p$ のとき，a は p の倍数である．1 と p^k の間の p の倍数の個数は，
p, $2p$, $3p$, …, $(p^{k-1}-2)p$, $(p^{k-1}-1)p$, p^k の p^{k-1} 個なので，$(a,\ p) = 1$ を満たす a の個数は，$p^k - p^{k-1}$.

(2) 集合 S, T と写像 $f : S \to T$ を以下のように定める．

$$S = \{a \mid a \text{ は } mn \text{ と互いに素な } mn \text{ 以下の自然数}\},$$
$$T = \{(b,\ c) \in \mathbb{N}^2 \mid b \text{ は } m \text{ と互いに素な } m \text{ 以下の自然数，} b \text{ は } n \text{ と互いに素な } n \text{ 以下の自然数}\}.$$

$a \in S$ に対して，$a \equiv b \pmod m$, $a \equiv c \pmod n$ を満たす $(b,\ c) \in T$ を対応させて，$f(a) = (b,\ c)$ とする．

$\forall (b,\ c) \in T$ に対して中国式剰余定理 (*4.7.2*) より，$a \equiv b \pmod m$, $a \equiv c \pmod n$ を満たす mn 以下の自然数 a がただ 1 つある．

$(b,\ m) = (c,\ n) = 1$ より $(a,\ mn) = 1$ となるから，$a \in S$ である．

f が全単射であることがわかったので，S と T の元の個数が等しい．ゆえに，$\varphi(mn) = \varphi(m)\varphi(n)$.

(3) (1) と (2) を用いると，$\varphi(n) = \varphi({p_1}^{e_1})\varphi({p_2}^{e_2})\cdots\varphi({p_r}^{e_r}) = ({p_1}^{e_1} - {p_1}^{e_1-1})({p_2}^{e_2} - {p_2}^{e_2-1})\cdots({p_r}^{e_r} - {p_r}^{e_r-1})$. ■

例 1

(1) $\varphi(42) = \varphi(2\cdot3\cdot7) = \varphi(2)\varphi(3)\varphi(7) = (2-1)(3-1)(7-1) = 12$.

(2) $\varphi(90) = \varphi(3^2\cdot2\cdot5) = (3^2-3)(2-1)(5-1) = 24$.

(3) $\varphi(8800) = \varphi(2^5\cdot5^2\cdot11) = (2^5-2^4)(5^2-5)(11-1) = 3200$.

5.2　オイラーの定理

オイラーの定理[17)]

n は自然数で，a は n と互いに素な整数とするとき，

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

特に，$n = p$ が素数のとき，

$$a^{p-1} \equiv 1 \pmod{p}.$$ (フェルマーの小定理)

証明：
$1 \leqslant b_1 < b_2 < \cdots < b_{\varphi(n)} < n$ を，1 と n の間にある n と互いに素な自然数とすると，
$ab_1, ab_2, \ldots, ab_{\varphi(n)}$ は n と互いに素である．($\because (a, n) = 1, (b_i, n) = 1 \Rightarrow (ab_i, n) = 1$.)
つまり，$ab_i \equiv b_{i'} \pmod{n}$ となる $1 \leqslant i \leqslant \varphi(n)$ がある．このとき，$ab_i \equiv ab_j \Rightarrow b_i \equiv b_j$ が成り立つ．($\because$ 両辺を a で割ればよい.)
すなわち，a をかけると $\{b_1, b_2, \ldots, b_{\varphi(n)}\}$ の置換 (全単射) がおこる．よって，

$$a^{\varphi(n)} b_1 b_2 \cdots b_{\varphi(n)} \equiv (ab_1)(ab_2)\cdots(ab_{\varphi(n)}) \equiv b_1 b_2 \cdots b_{\varphi(n)} \pmod{n}$$

の両辺を $b_1 b_2 \cdots b_{\varphi(n)}$ で割ると，$a^{\varphi(n)} \equiv 1 \pmod{n}$. ■

証明の中で $\star$ で割ると〜という表現を用いているが，$\star$ の**逆元**をかけるという．逆元を定義していないのであえて割るという表現をした．

定理３【１次合同式の解の 公 式】

n は自然数で，a, b は整数とする．a と n が互いに素ならば，１次合同式

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

は n を法としてただ１つ解をもち，それは

$$x = a^{\varphi(n)-1} b \pmod{n}$$

である．

証明：
オイラーの定理より，$ax \equiv a \cdot a^{\varphi(n)-1} b \equiv a^{\varphi(n)} b \equiv 1 \cdot b \equiv b \pmod{n}$. ■

例２
(1) $3x \equiv 2 \pmod{14}$
　$\varphi(14) = \varphi(2 \cdot 7) = \varphi(2)\varphi(7) = 6$. $x \equiv 3^{6-1} \cdot 2 \equiv 3^3 \cdot 3^2 \cdot 2 \equiv 13 \cdot 18 \equiv 13 \cdot 4 \equiv 10 \pmod{14}$.
(2) $5x \equiv 4 \pmod{12}$
　$\varphi(12) = \varphi(2^2 \cdot 3) = \varphi(2^2)\varphi(3) = 4$. $x \equiv 5^{4-1} \cdot 4 \equiv 5^2 \cdot 5 \cdot 4 \equiv 1 \cdot 5 \cdot 4 = 20 \equiv 8 \pmod{12}$.

[17)] オイラーの定理はフェルマーの小定理を一般化したものである．

5.3　暗号

暗号の用語

送信したいメッセージを **平文**（ひらぶん）という．
平文を第三者にわからない形にしたものを**暗号文**という．
平文を暗号文にする過程を**暗号化**という．暗号化の際に用いられる情報を**暗号化鍵**という．
暗号文を平文にする過程を**復号化**という．復号化の際に用いられる情報を**復号化鍵**という．
暗号化鍵を公開して誰でも利用できるような暗号を**公開鍵暗号**という．

例 3
アルファベット a,b,c,...,x,y,z,a,b,c,... を 1 だけずらして，平文を暗号化する．このような暗号を**シーザー暗号**という．
例えば，「apple」は「bqqmf」に暗号化される．アルファベットを 1 だけ前にずらして，暗号文を復号化する．この場合，暗号化鍵：+1，復号化鍵：−1．

5.4　RSA 暗号

RSA 暗号は，1977 年にリベスト (R.Rivest)，シャーミル (A.Sharmir)，エイドルマン (L.Adleman) が発表した暗号である．

暗号化鍵と復号化鍵

自然数 n, e, d を次の条件が成り立つように選ぶ．
(1) 相異なる素数 p, q を用いた $n = pq$．　(2) $\varphi(n) = (p-1)(q-1)$ と互いに素な e．　(3) $ed \equiv 1 \pmod{\varphi(n)}$ を満たす d．
(n, e) を**暗号化鍵 (公開鍵)**，d を**復号化鍵 (秘密鍵)** という．

暗号化

$0 \leqslant x < n$ を満たす整数 x を平文とする．

$$y \equiv x^e \pmod{n}$$

を満たす整数 y $(0 \leqslant y < n)$ を求める．y は x を暗号化してできる暗号文である．

復号化

暗号文 y に対して

$$z \equiv y^d \pmod{n}$$

を満たす整数 z $(0 \leqslant z < n)$ を求めると $z = x$ である．y から x に復号化される．

証明：
$ed \equiv 1 \pmod{\varphi(n)}$ より，$ed = 1 + \varphi(n)m$ を満たす整数 m がある．
(1) $(x, n) = 1$ の場合：オイラーの定理 (*5.2*) より，

$$z \equiv y^d \equiv (x^e)^d \equiv x^{1+\varphi(n)m} \equiv x \cdot (x^{\varphi(n)})^m \equiv x \cdot 1^m \equiv x \pmod{n}.$$

(2) $(x, n) \neq 1$ の場合：x は p または q の倍数である．$x = 0$ のとき，$z \equiv 0^{ed} \equiv 0 \pmod{n}$．次に $x \neq 0$ とする．
(i) x が p の倍数のとき，$x < n$ より $(x, q) = 1$ である．$x^{ed} - x$ は p の倍数なので，$x^{ed} \equiv x \pmod{p}$．$ed = 1 + \varphi(q)\varphi(p)m$ なので，
(1) と同様にオイラーの定理より，$x^{ed} \equiv x \cdot (x^{\varphi(q)})^{\varphi(p)m} \equiv x \cdot 1^{\varphi(p)m} \equiv x \pmod{q}$．　$\therefore z \equiv x^{ed} \equiv x \pmod{n}$.
(ii) x が q の倍数のとき，$x < n$ より $(x, p) = 1$．$x^{ed} - x$ は q の倍数なので，$x^{ed} \equiv x \pmod{q}$．$ed = 1 + \varphi(p)\varphi(q)m$ なので，
(i) と同様にオイラーの定理より，$x^{ed} \equiv x \pmod{p}$．よって $z \equiv x^{ed} \equiv x \pmod{n}$.
$0 \leqslant x, z < n$ で，$z - x$ は n の倍数だから，$z = x$．　■

➡**注** RSA 暗号を他人が復号化するには，$n = pq$ を素因数分解して，$\varphi(n) = (p-1)(q-1)$ と d を計算しないといけないが,p, q が巨大な数になると，$n = pq$ の素因数分解が困難になる．

5.5　RSA 暗号 例題

例題 次の暗号化鍵 (n, e) をもつ暗号文 y を解読せよ. 頻出 難

$$(n, e) = (51, 7),\ y = 2.$$

考え方 暗号化鍵 (n, e) から復号化鍵 d を求め，暗号文 y を復号化し，もとの平文 x を求める.

解答

$\varphi(n) = \varphi(51) = \varphi(3 \cdot 17) = \varphi(3)\varphi(17) = 2 \cdot 16 = 32$. $ed = 7d \equiv 1 \pmod{\varphi(n)} \equiv 1 \pmod{32}$ となる d を求める. オイラーの定理より，

$d \equiv 7^{\varphi(32)-1} \cdot 1 \equiv 7^{15} \equiv (7^4)^3 \cdot 7^3 \equiv 7^3 \equiv 343 \equiv 23 \pmod{32}$.　$\therefore d = 23$.

$y^d = 2^{23} \equiv (2^6)^3 \cdot 2^5 \pmod{n} \equiv 13^3 \cdot 2^5 \pmod{51} \equiv (13 \cdot 2^2)^2 \cdot 13 \cdot 2 \pmod{51} \equiv 1^2 \cdot 26 \pmod{51} \equiv 26 \pmod{51}$.　$\therefore x = 26$.

参考 答えがあっているか確かめる方法.

求めた x を暗号化して，y になれば o.k. つまり，$x^e \equiv y \pmod{n}$ であることを確認する.

例題に当てはめてみると，

$x^e = 26^7 = (26^2)^3 \cdot 26 \equiv 13^3 \cdot 26 \equiv (13^2 \cdot 26) \cdot 13 \equiv 8 \cdot 13 = 104 \equiv 2 \pmod{51} = y \pmod{51}$ になったので o.k.

演習 次の暗号化鍵 (n, e) をもつ暗号文 y を解読せよ. (復号化鍵 d と平文 x を求めよ.)

(1) $(n, e) = (34, 3),\ y = 32$　　(2) $(n, e) = (38, 5),\ y = 2$　　(3) $(n, e) = (65, 11),\ y = 2$

解答 (1) $d = 11,\ x = 26$　　(2) $d = 11,\ x = 34$　　(3) $d = 35,\ x = 33$

6　剰余類

6.1　既約剰余類

定義【既約剰余類】

2 以上の自然数 n と，整数 a に対して，a と n が互いに素であるとする．このとき，

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

を a が代表する**剰余類**，$a \pmod{n}$ を**既約な剰余類**という．**注** 代表の選び方によらない. (既約性)

例 1

4 を法とする剰余類は，

					代表							
$\cdots$	-8	$\sim$	-4	$\sim$	$\boxed{0}$	$\sim$	4	$\sim$	8	$\sim$	$\cdots$
$\cdots$	-7	$\sim$	-3	$\sim$	$\boxed{1}$	$\sim$	5	$\sim$	9	$\sim$	$\cdots$
$\cdots$	-6	$\sim$	-2	$\sim$	$\boxed{2}$	$\sim$	6	$\sim$	10	$\sim$	$\cdots$
$\cdots$	-5	$\sim$	-1	$\sim$	$\boxed{3}$	$\sim$	7	$\sim$	11	$\sim$	$\cdots$

の 4 つである．また，既約剰余類は $\cdots -7 \sim -3 \sim 1 \sim 5 \sim 9 \sim \cdots$, $\cdots -5 \sim -1 \sim 3 \sim 7 \sim 11 \sim \cdots$ である．

6.2　既約剰余類の位数

定義【位数】

$a \pmod{n}$ を既約剰余類とする．このとき，

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

となる最小の自然数 m を a の法 n における**位数** (order) という．記号として，

$$\mathrm{ord}_n(a) = m$$

と表す．

例 2

$n = 15$, $a = 2$ の場合：

$2^1 \equiv 2 \not\equiv 1 \pmod{15}$, $2^2 \equiv 4 \not\equiv 1 \pmod{15}$, $2^3 \equiv 8 \not\equiv 1 \pmod{15}$, $2^4 \equiv 16 \equiv 1 \pmod{15}$．$\therefore \mathrm{ord}_{15}(2) = 4$.

命題 1

k を正の整数，$(a, n) = 1$, $m = \mathrm{ord}_n(a)$ とする. このとき，

$$a^k \equiv 1 \pmod{n} \Longleftrightarrow m \mid k.$$

証明：

($\Leftarrow$)

$k = dm$ ($^\exists d \in \mathbb{Z}$) とすると，$a^k = a^{dm} \equiv (a^m)^d \equiv 1^d \equiv 1 \pmod{n}$.

($\Rightarrow$)

仮定より，$a^k \equiv 1 \pmod{n}$．$k = qm + r$ $(q \in \mathbb{Z}, 0 \leqslant r < m)$ とする.

$1 \equiv a^k \equiv a^{qm+r} \equiv a^{qm} \cdot a^r \equiv (a^m)^q \cdot a^r \equiv 1^q \cdot a^r \equiv a^r \pmod{n}$．$\therefore a^r \equiv 1 \pmod{n}$．ここで m の最小性より $r = 0$.

したがって $k = qm + 0 = qm$ と表せるので，k は m の倍数である．　■

問題 $n = 15$, $a = 8$ のときの位数を求めよ.

このような問題が出たとき，$8 (= 2^3)$ 程度であれば先ほどのように，1 つずつ確かめていけばよいのだが，a が例えば $1024 (= 2^{10})$ のときなどはとてもじゃないが，手計算ではしんどい．実は，そんな計算も簡単にできる公式がある．次のページで説明する.

命題 2 公式

k を正の整数，$(a, n) = 1$, $m = \mathrm{ord}_n(a)$ とする．このとき，次が成り立つ．

$$\mathrm{ord}_n(a^k) = \frac{m}{(k, m)}.$$

特に $(k, m) = 1$ のとき，$\mathrm{ord}_n(a^k) = \mathrm{ord}_n(a)$.

証明：

$(a^k)^{\frac{m}{(k, m)}} \equiv (a^m)^{\frac{k}{(k, m)}} \equiv 1^{\frac{k}{(k, m)}} \equiv 1 \pmod n$ なので，位数の最小性より，$\mathrm{ord}_n(a^k) \leqslant \frac{m}{(k, m)}$. …❶

次に，$\mathrm{ord}_n(a^k) = d$ $(\Leftrightarrow (a^k)^d = a^{kd} \equiv 1 \pmod n)$ $(\mathbb{N} \ni d \geqslant 1))$ とすると，

命題 1 (*6.2*) より，kd は m の倍数，すなわち $kd = \ell m$ となる整数 ℓ が存在する．

$kd = \ell m$ の両辺を (k, m) で割ると，$\frac{k}{(k, m)} \cdot d = \ell \cdot \frac{m}{(k, m)}$. $k' = \frac{k}{(k, m)}$, $m' = \frac{m}{(k, m)}$ とおくと，$(k', m') = 1$ なので，

ガウスの補題 (*2.4*) より，d は $m' = \frac{m}{(k, m)}$ の倍数である．つまり，$\frac{m}{(k, m)} \leqslant d = \mathrm{ord}_n(a^k)$. …❷

❶,❷より

$$\mathrm{ord}_n(a^k) \leqslant \frac{m}{(k, m)} \leqslant \mathrm{ord}_n(a^k).$$

これが意味することは，

$$\mathrm{ord}_n(a^k) = \frac{m}{(k, m)}.$$

である． ■

例 3

(1) $n = 15$, $a = 1024$ の場合：

例 2 より，$\mathrm{ord}_{15}(2) = 4$．また，$a = 1024 = 2^{10}$ なので，$(k, m) = (10, 4) = 2$ であるから，$\mathrm{ord}_{15}(1024) = \frac{4}{2} = 2$.

(2) $\mathrm{ord}_{15}(2^{99})$ を求める．

$(99, 4) = 1$ より，$\mathrm{ord}_{15}(2^{99}) = 4$.

6.3　オイラー関数の和公式

オイラー関数の定義は *5.1* を参照．オイラーの φ 関数を“剰余類”という言葉を使って言い換えると，

法 $n(\in \mathbb{N})$ の既約剰余類 $\Big[a \pmod n, (a, n) = 1 \Big]$ の個数を $\varphi(n)$ で表す．ただし $\varphi(1) := 1$.

オイラー関数の和公式

$$\sum_{d \mid n} \varphi(d) = n.$$

証明：

$(1 \leqslant) d$ を n の約数とする．$d' = \frac{n}{d}$ とおく．(かけて n になるものを d' とおいた．$dd' = n$.)

$1 \leqslant a \leqslant n$ の中で，$(a, n) = d'$ となるのものは $\varphi(d)$ 個である．

$\because$ $1 \leqslant b \leqslant d$ の中で，$(b, d) = 1$ となるものは $\varphi(d)$ 個である．(オイラー関数の定義より)
そのような b に対して，$(bd', n) = (bd', dd') = d'(b, d) = d'$. $a = bd'$ とおけば，成り立つ．逆に，$1 \leqslant a \leqslant n$ の中で，ある a が $(a, n) = d'$ を満たすならば，$\left(\frac{a}{d'}, \frac{n}{d'}\right) = 1 = \left(\frac{a}{d'}, d\right)$. $b = \frac{a}{d'}$ とおけば o.k. つまり，わかりやすく書くと，

$$\underset{\text{何個？}}{\{a \mid 1 \leqslant a \leqslant n, (a, n) = d'\}} \overset{\substack{d'\text{倍} \\ \leftrightarrows \\ \frac{1}{d'}\text{倍}}}{} \underset{\varphi(d)\text{ 個}}{\{b \mid 1 \leqslant b \leqslant d, (b, d) = 1\}}$$

$a \in \{1, 2, \ldots, n\}$ の中で，$(a, n) = d'$ なるものが $\varphi(d)$ 個．このように，d' の値によって，$\{1, 2, \ldots, n\}$ を分割し，足し合わせれば n になる．すなわち，それは

$$\sum_{d \mid n} \varphi(d) = n$$

を意味する． ■

6.4　原始根

a を法 n と既約な剰余類とする. ($(a, n) = 1$.) すると，オイラーの定理 (*5.2*) より，

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

が成り立つ. したがって，$\mathrm{ord}_n(a) \leqslant \varphi(n)$. *6.2* より，$\mathrm{ord}_n(a) \mid \varphi(n)$ が成り立つ.

特に，$n = p$(素数) のとき，$(a, p) = 1$ なので，既約剰余類は，$p-1$ 個 : $\varphi(p) = p-1$ である. したがって，$\mathrm{ord}_p(a) \mid p-1$.

今後は，特に断りがない限りは p は素数である.

定義【原始根】

p : 素数，既約剰余類 $a \pmod{p}$ の位数が $p-1$ であるとき，a は法 p の**原始根** (primitive roots) であるという.

例4　$p = 5, a = 3$ の場合 :

$3^1 = 3 \not\equiv 1 \pmod 5$, $3^2 = 9 \equiv 4 \not\equiv 1 \pmod 5$, $3^3 \equiv 4 \cdot 3 \equiv 12 \equiv 2 \not\equiv 1 \pmod 5$, $3^4 \equiv 2 \cdot 3 \equiv 6 \equiv 1 \pmod 5$.　$\therefore \mathrm{ord}_5(3) = 4 (= 5-1)$.

よって，3 は法 5 の原始根である.

補題 1

d : $p-1$ の約数とする.

位数 d の既約剰余類が 1 つでも存在すれば，$\varphi(d)$ 個ある.

証明 :

集合 A_d を次のように定める.

$$A_d := \{ b \mid \mathrm{ord}_p(b) = d \}$$　　(➪注 A_dの元は $b^d \equiv 1 \pmod p$ を満たす)

ここで b は方程式 $x^d \equiv 1 \pmod p$ の解である.

a を位数 d の元とすると，$1, a, \ldots, a^{d-1}$ は，$x^d \equiv 1 \pmod p$ の解のすべてである.[18] 特に $A_d \subset \{1, a, \ldots, a^{d-1}\}$.

$\{1, a, \ldots, a^{d-1}\}$ の中に A_d の元は $\varphi(d)$ 個ある (*6.3* の和公式の証明より). ■

定理 1

素数 p に対して，法 p の原始根は存在する.

証明 : $A_d := \{ b \mid \mathrm{ord}_n(b) = d \}$ とする. また，$\#X$ は集合 X の元の個数を表す.[19]

$\#A_d \neq 0$ であることを示せばよい.

$\sum_{d \mid p-1} \#A_d = p-1$ と $\sum_{d \mid p-1} \varphi(d) = p-1$ を見比べると，補題より，$\#A_d \neq 0 \Longrightarrow \varphi(d) = \#A_d$.

一方，$\varphi(d)$ は正なので，すべての $d \mid p-1$ に対して，$\#A_d = \varphi(d)$. ■

系 1

法 p の原始根は $\varphi(p-1)$ 個ある.

証明 :

原始根が存在するので，原始根 a をとる. このとき，$\{1, a, \ldots, a^{p-2}\}$ は法 p の既約剰余類全体である.[20] いま，$ord_p(a) = p-1$ なので，

$\mathrm{ord}_p(a^k) = \dfrac{p-1}{(k, p-1)}$　$(0 \leqslant k \leqslant p-2)$ である. a^k が原始根 $\Leftrightarrow (k, p-1) = 1$. そのような k は $\varphi(p-1)$ 個ある. ■

---

[18] **事実**として，「法 p (素数) における m 次方程式 $f(x) \equiv 0 \pmod p$ の解は高々 m 個 (m 個以下) である.」ということが知られている.
スマホか PC で「ラグランジュの定理 合同式」で検索すると出てくる (たぶん).

[19] 例えば，$A = \{x, y, z\}$ のとき，$\#A = 3$, $B = \{b_1, b_2, \ldots, b_n\}$ のとき，$\#B = n$.

[20] $\because a^i \equiv a^j \pmod p$ $(1 \leqslant i < j \leqslant p-2)$ とすると，$a^{j-i} \equiv 1 \pmod p$ $(1 \leqslant j-i \leqslant p-2)$ となり，a が原始根であることに反するから.

6.5　原始根の応用 n^2+1 の素因子

$n \in \mathbb{N}$ に対して，n^2+1 の素因子 (数) について考える．

1^2+1	$=$	2	6^2+1	$=$	37	11^2+1	$=$	$122 = 2\cdot 61$
2^2+1	$=$	5	7^2+1	$=$	$50 = 2\cdot 5^2$	12^2+1	$=$	$145 = 5\cdot 29$
3^2+1	$=$	$2\cdot 5$	8^2+1	$=$	$65 = 5\cdot 13$		$\cdot$	
4^2+1	$=$	17	9^2+1	$=$	$82 = 2\cdot 41$		$\cdot$	
5^2+1	$=$	$26 = 2\cdot 13$	10^2+1	$=$	101		$\cdot$	

定理 2

$n \in \mathbb{N}$, p：2 以外の素数 ($\overset{\text{def}}{\Longleftrightarrow}$ 奇素数) とする．

$$p \text{ が } n^2+1 \text{ の素因子として現れる．} \Longleftrightarrow p \equiv 1 \pmod 4.$$

証明：

p が n^2+1 の素因子である　$\Longleftrightarrow$　$n^2+1 = pk$　$(k \in \mathbb{Z})$

$\Longleftrightarrow$　$x^2+1 \equiv 0 \pmod p$ に解がある．

r を法 p の原始根のひとつとすると，原始根の定義より，$r^{\frac{p-1}{2}} \equiv -1 \pmod p$．(➡**注** p は奇数より $p-1$ は必ず偶数となる．)[21)]

($\Leftarrow$)

仮定より，$p = 4k+1 \Leftrightarrow k = \dfrac{p-1}{4}$ $(k \in \mathbb{Z})$．$n = r^{\frac{p-1}{4}}$ とおくと，$n^2 = r^{\frac{p-1}{2}} \equiv -1 \pmod p$．　$\therefore n^2 \equiv -1 \pmod p$．

したがって，$n^2+1 \equiv 0 \pmod p$．

($\Rightarrow$)

仮定より，$x^2+1 \equiv 0 \pmod p$ の解の存在性が保証されているので，

$x = r^{\frac{p-1}{4}}$ とすると，$x^2 = \left(r^{\frac{p-1}{4}}\right)^2 = r^{\frac{p-1}{2}} \equiv -1 \pmod p$ となるので，$r^{\frac{p-1}{4}}$ は解である．一方，$r^{\frac{p-1}{4}}$ が解であるためには，

$\dfrac{p-1}{4}$ が整数でなければならない．$\ell \in \mathbb{Z}$ として，$\ell = \dfrac{p-1}{4}$ と表すことにすると，$p = 4\ell+1 \Leftrightarrow p \equiv 1 \pmod 4$．　■

[21)] $\because r$ が原始根なので，$r^{p-1} \equiv 1 \pmod p \Leftrightarrow \left(r^{\frac{p-1}{2}}\right)^2 \equiv 1$．すなわち $r^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$．原始根は $p-1$ 乗ではじめて 1 になるので -1．

6.6　法 p の示数 (index)

定義【示数 (index)】

p：素数，r を原始根とする．このとき，

$$1,\ r,\ \ldots,\ r^{p-2}$$

は，法 p の既約剰余類のすべてである．($\{1, 2, \ldots, p-1\}$ の並び替え.) ゆえに，a を任意の既約剰余類とすると，

$$r^k \equiv a \pmod{p} \quad (0 \leqslant k \leqslant p-2)$$

とかける．(➡注 $r^k \equiv r^\ell \pmod{p} \Leftrightarrow k \equiv \ell \pmod{p-1}$．$p-1 = \mathrm{ord}_p(r)$.)
この $k \pmod{p-1}$ を a の原始根 r に関する**示数**という．記号として，

$$\mathrm{ind}_r(a) \equiv k \pmod{p-1}$$

とかく．

命題３

$n \in \mathbb{N}$, r を原始根，a, b を既約剰余類とする．このとき，次が成り立つ．
(1) $\mathrm{ind}_r(ab) = \mathrm{ind}_r(a) + \mathrm{ind}_r(b)$.　(2) $\mathrm{ind}_r(a^n) = n\,\mathrm{ind}_r(a)$.　(3) $\mathrm{ind}_r(r) = 1$, $\mathrm{ind}_r(1) = 0$.

証明：
$\mathrm{ind}_r(a) = k$, $\mathrm{ind}_r(b) = \ell$ とする．
(1) $ab \equiv r^k \cdot r^\ell \equiv r^{k+\ell} \pmod{p}$．　$\therefore \mathrm{ind}_r(ab) = k + \ell = \mathrm{ind}_r(a) + \mathrm{ind}_r(b)$.
(2) $a^n \equiv (r^k)^n \equiv r^{nk} \pmod{p}$．　$\therefore \mathrm{ind}_r(a^n) = nk = n\,\mathrm{ind}_r(a)$.
(3) $r \equiv r^1 \pmod{p}$．　$\therefore \mathrm{ind}_r(r) = 1$, $1 \equiv r^0 \pmod{p}$．　$\therefore \mathrm{ind}_r(1) = 0$.　■

例５
$p = 13$, $r = 2$ の場合：
$2^1 \equiv 2 \pmod{13}$, $2^2 \equiv 4 \pmod{13}$, $2^3 \equiv 8 \pmod{13}$, $2^4 \equiv 16 \equiv 3 \pmod{13}$, $2^5 \equiv 2^4 \cdot 2 \equiv 3 \cdot 2 \equiv 6 \pmod{13}$, $2^6 \equiv 12 \pmod{13}$,
$2^7 \equiv 24 \equiv 11 \pmod{13}$, $2^8 \equiv 22 \equiv 9 \pmod{13}$, $2^9 \equiv 18 \equiv 5 \pmod{13}$, $2^{10} \equiv 10 \pmod{13}$, $2^{11} \equiv 20 \equiv 7 \pmod{13}$, $2^{12} \equiv 14 \equiv 1 \pmod{13}$.
つまり，2 は法 13 の原始根である．これらの計算から，

a	1	2	3	4	5	6	7	8	9	10	11	12	← mod 13 の世界
$\mathrm{ind}_2(a)$	0	1	4	2	9	5	11	3	8	10	7	6	← mod 12 の世界

がかける．この表のことを**示数表**という．示数表を用いると次のような計算が簡単にできる．

計算例

(1) $x^7 \equiv 5 \pmod{13}$
両辺の示数をとると，$\mathrm{ind}_2(x^7) \equiv \mathrm{ind}_2(5) \pmod{12}$．示数表より，$7\mathrm{ind}_2(x) \equiv 9 \pmod{12}$.
$y = \mathrm{ind}_2(x)$ とでもおけば $7y \equiv 9 \pmod{12}$ を解けばよい．この解き方はいろいろあるので任せる．(**ヒント**：7 の逆元を両辺にかけたりする.)
$7y \equiv 9 \pmod{12} \Leftrightarrow y \equiv -5 \cdot 9 = -45 \equiv 3 \pmod{12}$．　$\therefore y = \mathrm{ind}_2(x) \equiv 3 \pmod{12}$．示数表より，$x \equiv 8 \pmod{13}$.
Check! $x^7 = 8^7 \equiv (2^3)^7 \equiv 2^{21} \equiv (2^4)^5 \cdot 2 \equiv 3^5 \cdot 2 \equiv 3^3 \cdot 3^2 \cdot 2 \equiv 3^2 \cdot 2 \equiv 18 \equiv 5 \pmod{13}$ なので o.k.

(2) $x^3 \equiv 12 \pmod{13}$
両辺の示数をとると，$3\mathrm{ind}_2(x) \equiv \mathrm{ind}_2(12) \pmod{12} \Leftrightarrow 3\mathrm{ind}_2(x) \equiv 6 \pmod{12} \Leftrightarrow \mathrm{ind}_2(x) \equiv 2 \pmod{4}$.
$\therefore \mathrm{ind}_2(x) \equiv 2, 6, 10 \pmod{12}$．示数表より，$x \equiv 4, 12, 10 \pmod{13}$.

(3) $x^2 + 9x + 7 \equiv 0 \pmod{13}$
$x^2 + 9x + 7 \equiv x^2 - 4x + 7 = (x-2)^2 - 2^2 + 7 \equiv (x-2)^2 + 3 \pmod{13} \Leftrightarrow (x-2)^2 \equiv -3 \equiv 10 \pmod{13}$.
両辺の示数をとると，$2\mathrm{ind}_2(x-2) \equiv \mathrm{ind}_2(10) \pmod{12} \Leftrightarrow 2\mathrm{ind}_2(x-2) \equiv 10 \pmod{12} \Leftrightarrow \mathrm{ind}_2(x-2) \equiv 5 \pmod{6}$.
$\therefore \mathrm{ind}_2(x-2) \equiv 5, 11 \pmod{12}$．示数表より，$x - 2 \equiv 6, 7 \pmod{13} \Leftrightarrow x \equiv 8, 9 \pmod{13}$.

演習 次の問いに答えよ．

1. 3 は法 17 における原始根であることを示し，示数表を完成させよ．

2. 示数表を用いて以下の方程式を解け．
(1) $x^2 + 7x + 5 \equiv 0 \pmod{17}$　(2) $x^2 + 3x + 11 \equiv 0 \pmod{17}$　(3) $x^4 \equiv 13 \pmod{17}$

解 **1**. 略．**2**. (1) 解なし．　(2) $x \equiv 5, 9 \pmod{17}$.　(3) $x \equiv 3, 5, 14, 12 \pmod{17}$.

6.7　平方剰余

$ax^2+bx+c=0$ $(a, b, c \in \mathbb{R}, a \neq 0)$ において，

$$0=ax^2+bx+c=a\left(x^2+\frac{b}{a}x\right)+c=a\left\{\left(x+\frac{b}{2a}\right)^2-\frac{b^2}{4a^2}\right\}+c \Leftrightarrow a\left(x+\frac{b}{2a}\right)^2-\frac{b^2}{4a}=-c \Leftrightarrow \left(x+\frac{b}{2a}\right)^2=\frac{b^2-4ac}{4a^2} \quad \therefore x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}.$$

このとき，実数根の個数の判別として，判別式 $D:=b^2-4ac$ を用いて，

$$\begin{array}{lll} D>0 & \Longrightarrow & D \text{ の平方根が 2 つ} \Leftrightarrow \text{実数根をもつ.} \\ D=0 & \Longrightarrow & \text{重根} \\ D<0 & \Longrightarrow & \text{実数根なし.} \end{array}$$

とできた．これを合同式の場合で考えたい．

つまり，a, b, c を整数，p：奇素数を法とする．ただし，$a \not\equiv 0 \pmod{p}$．このとき，

$$\left(x+\frac{b}{2a}\right)^2=\frac{b^2-4ac}{4a^2}$$

までを考えればよい．法 p の世界では正・負に意味はない．なぜならば，法 p の世界では，正は負に，負は正にできるからである．

この場合，法 p の原始根 r を使って“判別”した．

定義【平方剰余】

p：奇素数，a を法 p の既約剰余類とする．このとき，

$$x^2 \equiv a \pmod{p}$$

が整数解をもつとき，a を法 p の**平方剰余**といい，もたない場合，a を法 p の**非平方剰余**という．略して，平方，非平方ともいう．

例 6

(1) $p=3$ の場合：

a	1	2
a^2	1	1

（← mod 3 の世界）なので，平方：1，非平方：2.

(2) $p=5$ の場合：

a	1	2	3	4
a^2	1	4	4	1

（← mod 5 の世界）なので，平方：1, 4，非平方：2, 3.

(3) $p=7$ の場合：

a	1	2	3	4	5	6
a^2	1	4	2	2	4	1

なので，平方：1, 2, 4，非平方：3, 5, 6.

(4) $p=11$ の場合：

a	1	2	3	4	5	6	7	8	9	10
a^2	1	4	9	5	3	3	5	9	4	1

なので，平方：1, 3, 4, 5, 9，非平方：2, 6, 7, 8, 10.

命題 4

p：奇素数，$a \not\equiv 0 \pmod{p}$, r：法 p の原始根とする．このとき，

$$a \text{ が平方剰余} \Longleftrightarrow \mathrm{ind}_r(a) \text{ が偶数.}$$

特に，平方剰余と非平方剰余が $\frac{p-1}{2}$ 個ずつある．[22)]

<u>証明：</u>

仮定より，$x^2 \equiv a \pmod{p}$ に解がある．両辺の示数をとると，$2\mathrm{ind}_r(x) \equiv \mathrm{ind}_r(a) \pmod{p-1}$.

ここで p は奇素数なので，$p-1$ は偶数である．また左辺は 2 がかかっているので偶数である．

よって，これが解をもつためには $\mathrm{ind}_r(a)$ が偶数でなければならない．したがって，

$$a \text{ が平方剰余} \overset{\text{def}}{\Longleftrightarrow} x^2 \equiv a \pmod{p} \text{ が解をもつ} \Longleftrightarrow \mathrm{ind}_r(a) \text{ が偶数}$$

であることが示せた． ■

➡**注** $\mathrm{ind}_r(a)$ の偶奇は r の選び方によらない．

[22)] $\mathrm{ind}_r(a)$ は mod $p-1$(偶数) の世界なので，半分が偶数，もう半分が奇数なので，そのうち偶数が平方なので，残り半分が非平方になることがわかる．

6.8　ルジャンドルの記号

定義【ルジャンドル (**Legendre**) の記号】

p：奇素数, $a \not\equiv 0 \pmod{p}$ のとき,

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & (a \text{ が法 } p \text{ で平方剰余}) \\ -1 & (a \text{ が法 } p \text{ で非平方剰余}) \end{cases}$$

➡注 $a \equiv b \pmod{p}$ のとき, $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

例 6′

(1) $p = 3$ の場合：　$\left(\frac{1}{3}\right) = 1, \left(\frac{2}{3}\right) = -1.$

(2) $p = 5$ の場合：　$\left(\frac{1}{5}\right) = 1, \left(\frac{2}{5}\right) = -1, \left(\frac{3}{5}\right) = -1, \left(\frac{4}{5}\right) = 1.$

6.9　オイラーの規準，第 1 補充法則

オイラーの規準 (**Euler's criterion**)

p：奇素数，$a \not\equiv 0 \pmod{p}$ とする．このとき，

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

証明：

$x^{p-1} - 1 \equiv 0 \pmod{p}$ の解は $p-1$ 個ある．いま，p は奇数より $p-1$ は偶数なので，$\left(x^{\frac{p-1}{2}} + 1\right)\left(x^{\frac{p-1}{2}} - 1\right) \equiv 0 \pmod{p}$.

つまり，$x^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}$ または $x^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$ である．*6.7* の命題 4 より，これらは半分ずつある．

r を原始根，a を平方剰余であるとすると，*6.7* の命題 4 より，$a \equiv r^{2k} \pmod{p}$ $(k \in \mathbb{N})$ とできる．このとき，

$a^{\frac{p-1}{2}} \equiv r^{2k \cdot \frac{p-1}{2}} \equiv r^{k(p-1)} \equiv 1 \pmod{p}$ なので，$x = a$ は $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ を満たすので解である．[23)]

a が非平方剰余であるとすると，$a \equiv r^{2k+1} \pmod{p}$ $(k \in \mathbb{N})$ とかける．前述と同様の議論をすると，

$a^{\frac{p-1}{2}} \equiv r^{(2k+1)\left(\frac{p-1}{2}\right)} \equiv r^{k(p-1)} \cdot r^{\frac{p-1}{2}} \equiv 1 \cdot r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. (原始根の最小性より．詳しくは *6.5* の定理 2 の証明の注釈を参照.)

よって，$x = a$ は $x^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ の解である．　■

系 2 (乗法性)

p：奇素数，$a, b \not\equiv 0 \pmod{p}$ とする．このとき，次が成り立つ．

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

証明：

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$ ■

系 3 【ガウスの第 1 補充法則】

p：奇素数とする．次が成り立つ．

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & p \equiv 1 \pmod{4} \\ -1 & p \equiv 3 \pmod{4} \end{cases}.$$

証明：

$p \equiv 1 \pmod{4} \Leftrightarrow p = 4k+1$ $(k \in \mathbb{Z})$. $\frac{p-1}{2} = \frac{4k}{2} = 2k$. $p \equiv 3 \pmod{4} \Leftrightarrow p = 4k+3$. $\frac{p-1}{2} = \frac{4k+2}{2} = 2k+1$.　■

[23)] r が原始根なので，$r^{p-1} \equiv 1 \pmod{p}$ であるから，$r^{k(p-1)} = (r^{p-1})^k \equiv 1^k \equiv 1 \pmod{p}$ となる．

6.10　ガウスの補題 [平方剰余]，第 2 補充法則

ガウスの補題 [平方剰余][24)]

p：奇素数とする．法 p の既約剰余類を

$$S_p=\left\{1,\,2,\,\cdots,\,\frac{p-1}{2}\right\}\text{とおく．ただし，}-S_p=\left\{-1,\,-2,\,\cdots,\,-\frac{p-1}{2}\right\}\qquad(*1)$$

法 p の既約剰余類は $S_p\cup -S_p$ で代表される．(➡**注** $S_p\cap -S_p=\varnothing$.) $s\in S_p$ と $a\not\equiv 0\pmod p$ に対して，

$$as\equiv\varepsilon_s(a)s_a,\quad \varepsilon_s(a)=\{+1,\,-1\},\quad s_a\in S_p\qquad(*2)$$

とかく．このとき，次が成り立つ．

$$\left(\frac{a}{p}\right)=\prod_{s\in S_p}\varepsilon_s(a).$$

<u>証明：</u>

$S_p\ni s\mapsto s_a\in S_p$ は全単射なので，$as\equiv\varepsilon_s(a)s_a$ をすべてにわたってかける．

$$\prod_{s\in S_p}(as)\equiv\prod_{s\in S_p}\varepsilon_s(a)s_a\qquad\cdots\cdots\cdots\cdots\cdots\cdots①$$

$$a^{\frac{p-1}{2}}\cdot\prod_{s\in S_p}s\equiv\prod_{s\in S_p}\varepsilon_s(a)\cdot\prod_{s\in S_p}s_a\qquad\cdots\cdots\cdots\cdots\cdots\cdots②$$

$$a^{\frac{p-1}{2}}\cdot\prod_{s\in S_p}s\equiv\prod_{s\in S_p}\varepsilon_s(a)\cdot\prod_{s\in S_p}s\qquad\cdots\cdots\cdots\cdots\cdots\cdots③$$

$$a^{\frac{p-1}{2}}\equiv\prod_{s\in S_p}\varepsilon_s(a)\qquad\cdots\cdots\cdots\cdots\cdots\cdots④$$

① から ② は a は S_p の元が $\dfrac{p-1}{2}$ 個あるから．② から ③ は $s\mapsto s_a$ が全単射なので．③ から ④ は両辺を $\prod_{s\in S_p}s$ で割った．

6.9 のオイラーの規準より，$a^{\frac{p-1}{2}}\equiv\left(\dfrac{a}{p}\right)$ なので，

$$\left(\frac{a}{p}\right)=\prod_{s\in S_p}\varepsilon_s(a).\qquad\blacksquare$$

第 2 補充法則

p：奇素数とする．

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=\begin{cases}+1 & p\equiv\pm1\pmod 8\\ -1 & p\equiv\pm5\pmod 8\end{cases}$$

<u>証明：</u> $\varepsilon_s(2)$ を考える．

$2s>\dfrac{p}{2}\Leftrightarrow s>\dfrac{p}{4}\Leftrightarrow\varepsilon_s(2)=-1$．よって，$\left(\dfrac{2}{p}\right)=(-1)^{\frac{p-1}{2}-\left[\frac{p}{4}\right]}$．([b] はガウス記号と呼ばれ，b を超えない最大の整数を表す.)

- $p\equiv1\pmod 8$ のとき，$p=8k_1+1\Rightarrow\dfrac{p-1}{2}-\left[\dfrac{p}{4}\right]=4k_1-\left[2k_1+\dfrac{1}{4}\right]=4k_1-2k_1=2k_1\quad(k_1\in\mathbb{Z})$.
- $p\equiv-1\pmod 8$ のとき，$p=8k_2-1\Rightarrow\dfrac{p-1}{2}-\left[\dfrac{p}{4}\right]=4k_2-1-\left[2k_2-\dfrac{1}{4}\right]=4k_2-2k_2=2k_2\quad(k_2\in\mathbb{Z})$.
- $p\equiv5\pmod 8$ のとき，$p=8\ell_1+5\Rightarrow\dfrac{p-1}{2}-\left[\dfrac{p}{4}\right]=4\ell_1+2-\left[2\ell_1+\dfrac{5}{4}\right]=4\ell_1-2\ell+2-1=2\ell_1+1\quad(\ell_1\in\mathbb{Z})$.
- $p\equiv-5\pmod 8$ のとき，$p=8\ell_2-5\Rightarrow\dfrac{p-1}{2}-\left[\dfrac{p}{4}\right]=4\ell_2-3-\left[2\ell_2-\dfrac{5}{4}\right]=4\ell_2-2\ell_2-3+2=2\ell_2-1\quad(\ell_2\in\mathbb{Z})$.

したがって，結論を得る．$\blacksquare$

[24)] (*1) の例：mod 7 のとき $\{1,2,3,4,5,6\}$ は $\{1,2,3,-3,-2,-1\}$ ともかける．このとき，$S_7=\{1,2,3\}$, $-S_7=\{-1,-2,-3\}$ である．

(*2) の例：

s_a	1	2	3
$\varepsilon_s(a)$	-1	$+1$	-1
s	3	1	2

6.11　平方剰余の相互法則

平方剰余の相互法則

p, q：相異なる奇素数とする．次が成り立つ．

$$\left(\frac{q}{p}\right)\cdot\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

証明：

$f_p(x)=\sin\dfrac{2\pi x}{p}$　$(x\in\mathbb{Z})$ とおく．すると，次が成り立つ．

(i) $f_p(x+p)=f_p(x)$．　(ii) $s\in S_p\Rightarrow f_p(s)>0$ $(f_p(-s)=-f_p(s)<0)$．

(i) より，$\mathbb{Z}\ni x\pmod p$ で代入することに意味がある．(2π が周期なので．) また，(ii) より，$f_p(as)$ の符号 $=\varepsilon_s(a)$．

記号として

$$\mathrm{sgn}(a):=\begin{cases}+1 & (a>0)\\ -1 & (a<0)\end{cases}$$

を使う．つまり，$\mathrm{sgn}\Big(f_p(as)\Big)=\varepsilon_s(a)$．この証明をするために，次の公式を用いる．

公 式

$n\geqslant 3$ 以上の奇数とする．

$$\sin(nx)=2^{n-1}\sin x\prod_{j=1}^{(n-1)/2}\left(\sin^2\frac{2\pi j}{n}-\sin^2 x\right)$$

$$\begin{aligned}
\left(\frac{q}{p}\right)&=\prod_{s\in S_p}\mathrm{sgn}\Big(f_p(qs)\Big) && \cdots\cdots\cdots\cdots\cdots\cdots ①\\
&=\mathrm{sgn}\left(\prod_{s\in S_p}\sin\frac{2\pi qs}{p}\right) && \cdots\cdots\cdots\cdots\cdots\cdots ②\\
&=\mathrm{sgn}\left(\prod_{s\in S_p}\left(2^{q-1}\sin\frac{2\pi s}{p}\prod_{j=1}^{(q-1)/2}\left(\sin^2\frac{2\pi j}{q}-\sin^2\frac{2\pi s}{p}\right)\right)\right) && \cdots\cdots\cdots\cdots\cdots\cdots ③\\
&=\mathrm{sgn}\left(\prod_{s\in S_p}\left(\prod_{j=1}^{(q-1)/2}\left(\sin^2\frac{2\pi j}{q}-\sin^2\frac{2\pi s}{p}\right)\right)\right) && \cdots\cdots\cdots\cdots\cdots\cdots ④\\
&=\mathrm{sgn}\left(\prod_{s=1}^{(p-1)/2}\prod_{j=1}^{(q-1)/2}\left(\sin^2\frac{2\pi j}{q}-\sin^2\frac{2\pi s}{p}\right)\right) && \cdots\cdots\cdots\cdots\cdots\cdots ⑤
\end{aligned}$$

① から ② は $\pm$ の積なので入れ替え可能と $f_p(qs)$ を代入した．② から ③ は q を n，$\dfrac{2\pi s}{p}$ を x だと思って，公式に代入した．

③ から ④ は $2^{q-1}\sin\dfrac{2\pi s}{p}>0$ で符号だけを考えればよいので省略した．④ から ⑤ は集合 S_p の定義より．

同様にして，

$$\left(\frac{p}{q}\right)=\mathrm{sgn}\left(\prod_{j=1}^{(q-1)/2}\prod_{s=1}^{(p-1)/2}\left(\sin^2\frac{2\pi s}{p}-\sin^2\frac{2\pi j}{q}\right)\right)$$

となる．$p'=\sin^2\dfrac{2\pi s}{p}$, $q'=\sin^2\dfrac{2\pi j}{q}$ とおくと，

$$\left(\frac{q}{p}\right)=\mathrm{sgn}\left(\prod_{s=1}^{(p-1)/2}\prod_{j=1}^{(q-1)/2}(q'-p')\right),\ \left(\frac{p}{q}\right)=\mathrm{sgn}\left(\prod_{j=1}^{(q-1)/2}\prod_{s=1}^{(p-1)/2}(p'-q')\right)$$

つまり，$\left(\dfrac{p}{q}\right)=\mathrm{sgn}\left(\displaystyle\prod_{j=1}^{(q-1)/2}\prod_{s=1}^{(p-1)/2}(-1)\cdot(q'-p')\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\cdot\mathrm{sgn}\left(\displaystyle\prod_{s=1}^{(p-1)/2}\prod_{j=1}^{(q-1)/2}(q'-p')\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\dfrac{q}{p}\right)$．

したがって，

$$\left(\frac{q}{p}\right)\cdot\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

■

演習

1. $\left(\frac{91}{1109}\right)$ を求めよ.

2. 次の合同方程式に解が存在するかどうかを調べよ. $x^2+9x+51\equiv 0 \pmod{71}$.

解 答

1. $\left(\frac{91}{1109}\right)=\left(\frac{7}{1109}\right)\left(\frac{13}{1109}\right)=\left(\frac{1109}{7}\right)\left(\frac{1109}{13}\right)=\left(\frac{3}{7}\right)\left(\frac{4}{13}\right)=-\left(\frac{7}{3}\right)\left(\frac{2}{13}\right)\left(\frac{2}{13}\right)=-\left(\frac{1}{3}\right)(-1)\cdot(-1)=-1.$

2.

考え方１.

平方完成し，整理した右辺の数が平方かどうかを調べる．平方 (剰余) なら解は存在，非平方なら解なし.

解答：

$x^2+9x+51\equiv x^2-62x+51=(x-31)^2-961+51\equiv(x-31)^2-58\equiv 0\Leftrightarrow(x-31)^2\equiv 58 \pmod{71}$.

$\left(\frac{58}{71}\right)=\left(\frac{2\cdot 29}{71}\right)$ 乗法性より

$=\left(\frac{2}{71}\right)\cdot\left(\frac{29}{71}\right)$ $71\equiv -1 \pmod 8$ なので第 2 補充法則より

$=(+1)\cdot\left(\frac{29}{71}\right)$ 相互法則より

$=\left(\frac{71}{29}\right)=\left(\frac{13}{29}\right)$ 相互法則より

$=\left(\frac{29}{13}\right)=\left(\frac{3}{13}\right)$ 相互法則より

$=\left(\frac{13}{3}\right)=\left(\frac{1}{3}\right)=1.$ $\therefore\left(\frac{58}{71}\right)=1$ なので 58 は平方である．したがって解は存在する.

考え方２.

判別式 $D(=b^2-4ac)$ が平方かどうかを調べる．平方なら解あり，非平方なら解なし.

解答：

$D=81-204=-123\equiv 19 \pmod{17}$

$\left(\frac{19}{71}\right)$ 相互法則より (19 − 1, 71 − 1 は 2 でわると奇数になるので − がつく)

$=-\left(\frac{71}{19}\right)=-\left(\frac{14}{19}\right)=-\left(\frac{2\cdot 7}{19}\right)$ 乗法性より

$=-\left(\left(\frac{2}{19}\right)\cdot\left(\frac{7}{19}\right)\right)$ $19\equiv 3\equiv -5 \pmod 8$ なので第 2 補充法則より

$=-\left((-1)\cdot\left(\frac{7}{19}\right)\right)=\left(\frac{7}{19}\right)$ 相互法則より

$=-\left(\frac{19}{7}\right)=-\left(\frac{5}{7}\right)$ 相互法則より

$=-\left(\frac{7}{5}\right)=-\left(\frac{2}{5}\right)$ 第 2 補充法則より

$=-(-1)=1.$ $\therefore\left(\frac{19}{71}\right)=1.$ よって解は存在する.

第 II 部

代数学入門の入門

7　集合の関係

7.1　2 項関係

“＝”（イコール, equal) が持っている性質

(i) $a = a$.　　(ii) $a = b$ ならば，$b = a$.　　(iii) $a = b$ かつ $b = c$ ならば，$a = c$.

(i) のことを**反射律**，(ii) のことを**対称律**，(iii) のことを**推移律**という．a, b, c はある集合 X の元と考える．

イコールと似たもの

例 1

$X = \mathbb{Z}$ として，自然数 n を 1 つ選ぶ．このとき，$a \equiv b \pmod{n}$ は (i),(ii),(iii) を満たす．

このように，イコールの持っている性質を一般化していこうと思うわけである．

定義【直積集合】

2 つの“もの”a, b から作られた対 (a, b) を，a と b から作られた**順序対**という．2 つの順序対 (a, b) と (a', b') が等しいのは，$a = a'$ かつ $b = b'$ がともに成り立つ場合に限るとする．

集合 A, B に対して，A の元 a と B の元 b とから作られる順序対 (a, b) の全体からなる集合を A と B の**直積**といい，$A \times B$ で表す．

A を任意の集合とする．

“＝”は $A \times A$ の部分集合 $R = \{(a, b) \in A \times A \,|\, a = b\} = \{(a, a) \in A \times A \,|\, a \in X\} \subset A \times A$ とかける．

このとき，部分集合 R は「$(a, b) \in R \Longleftrightarrow a = b$ を定める」とかく.[25)]

定義【2 項関係】

任意の集合 A に対して，その直積 $A \times A$ の任意の部分集合 R のことを A 上の**2 項関係**という．

➡**注** “＝”だけが 2 項関係ではない．

例 2

(1) $A = \mathbb{R}$ としたとき，$R = \{(a, b) \in \mathbb{R}^2 \,|\, a \leqslant b\}$ は 2 項関係.　　(2) $A = \mathbb{R}$ としたとき，$R = \{(a, b) \in \mathbb{R}^2 \,|\, a^2 < b\}$ は 2 項関係.

つまり，a と b に何かしらの“関係”があれば，それは 2 項関係である．

7.2　同値関係

定義【同値関係 (equivalence relation)】

任意の集合 A 上の 2 項関係 R が**同値関係**であるとは，以下の 3 つの条件が成立することである．

（ i ）**反射律**　任意の $a \in A$ に対して，$(a, a) \in A$.

（ ii ）**対称律**　$(a, b) \in R \Longrightarrow (b, a) \in R$.

（iii）**推移律**　$(a, b) \in R$ かつ $(b, c) \in R \Longrightarrow (a, c) \in R$.

また，A 上の同値関係 (の候補)R が与えられたとき，$(a, b) \in R$ を $a \sim b$ とかく．

例 2′

(1) は同値関係ではない．（ ii ）が不成立である．

($\because (a, b) \in R \overset{\text{def}}{\Longleftrightarrow} a \leqslant b$ なので $a = 1, b = 2$ とすると，$a = 1 \leqslant 2 = b$ だが，$b = 2 \not\leqslant 1 = a \Leftrightarrow (b, a) \notin R$.)

(2) も同値関係ではない．

例 3

(1) $\mathbb{R}^2$ 上の二項関係を $(a, b) \sim (c, d) \overset{\text{def}}{\Longleftrightarrow} a^2 + b^2 = c^2 + d^2$ は同値関係である．

（ i ）$a^2 + b^2 = a^2 + b^2 \Rightarrow (a, b) \sim (a, b)$ なので o.k.

（ ii ）$(a, b) \sim (c, d) \Leftrightarrow a^2 + b^2 = c^2 + d^2 \Leftrightarrow c^2 + d^2 = a^2 + b^2 \Leftrightarrow (c, d) \sim (a, b)$ なので o.k.

（iii）$(a, b) \sim (c, d)$ かつ $(c, d) \sim (e, f) \Leftrightarrow a^2 + b^2 = c^2 + d^2$かつ $c^2 + d^2 = e^2 + f^2 \Rightarrow a^2 + b^2 = c^2 + d^2 = e^2 + f^2$

$\Leftrightarrow a^2 + b^2 = e^2 + f^2 \Leftrightarrow (a, b) \sim (e, f)$ なので o.k.

[25)] 略して $(a, b) \in R \overset{\text{def}}{\Longleftrightarrow} a = b$ ともかく．

7.3　同値類

定義【同値類 (equivalence class)】

集合 A 上に同値関係 $\sim$ が与えられているとする. $(R = \{(x, y) \in A \times A \,|\, x \sim y\})$ このとき，任意の $a \in A$ に対して，

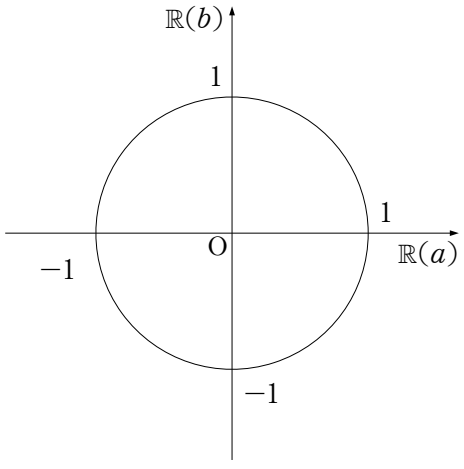
$$C(a) := \{b \in A \,|\, a \sim b\}$$

を a が定める**同値類**という．➡**注** $a \in C(a)$ $(\because a \sim a$ より$)$．特に，$C(a) \neq \varnothing$.

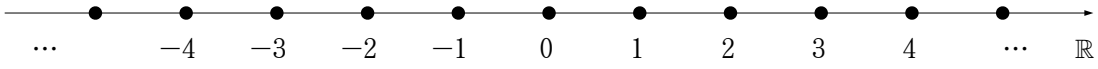
例 4

(1) $\mathbb{R}^2$ 上の同値関係 $(a, b) \sim (c, d) \overset{\text{def}}{\iff} a^2 + b^2 = c^2 + d^2$ の同値類 $C\Big((1, 0)\Big)$ は，$C\Big((1, 0)\Big) = \{(a, b) \in \mathbb{R}^2 | (1, 0) \sim (a, b)\}$ なので

$(1, 0) \sim (a, b) \Leftrightarrow 1^2 + 0^2 = a^2 + b^2 \Leftrightarrow a^2 + b^2 = 1$ となるから，同値類 $C\Big((1, 0)\Big)$ は，原点中心，半径 1 の円である.

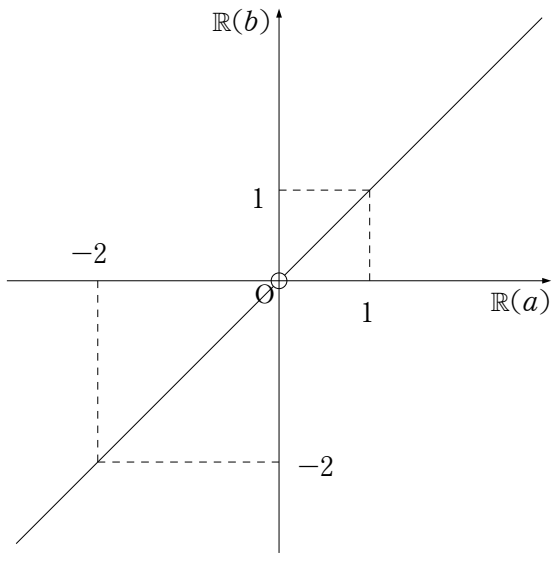


(2) $\mathbb{R}$ 上の同値関係 $a \sim b \overset{\text{def}}{\iff} a - b \in \mathbb{Z}$ の同値類 $\mathrm{C}(0)$ は，$\mathrm{C}(0) = \{a \in \mathbb{R} | 0 \sim a\}$ なので，$0 \sim a \Leftrightarrow 0 - a \in \mathbb{Z} \Leftrightarrow a \in \mathbb{Z}$ である.



(3) $\mathbb{R}^2 \backslash \{(0, 0)\}$ 上の同値関係 $(a, b) \sim (c, d) \overset{\text{def}}{\iff} (a, b) = t(c, d)$ $(^\exists t \in \mathbb{R} \backslash \{0\})$ の同値類 $\mathrm{C}((1, 1))$ は，

$\mathrm{C}((1, 1)) = \{(a, b) \in \mathbb{R}^2 | (1, 1) \sim (a, b)\}$ なので，$(1, 1) \sim (a, b) \Leftrightarrow (1, 1) = t(a, b) \Leftrightarrow ta = tb \Leftrightarrow a = b$. よって傾き 1 の直線となる.



図より (1) の同値類は円，(2) の同値類は点列，(3) の同値類は直線になることがわかる.[26)]

演習 次の同値類を作図せよ.

(1) $\mathbb{R}^2$ 上の同値関係 $(a, b) \sim (c, d) \overset{\text{def}}{\iff} a^2 + b^2 = c^2 + d^2$ の同値類 $\mathrm{C}((1, 1))$.

(2) $\mathbb{R}$ 上の同値関係 $a \sim b \overset{\text{def}}{\iff} a - b \in \mathbb{Z}$ の同値類 $\mathrm{C}\left(\frac{1}{2}\right)$.

(3) $\mathbb{R}^2 \backslash \{(0, 0)\}$ 上の同値関係 $(a, b) \sim (c, d) \overset{\text{def}}{\iff} (a, b) = t(c, d)$ $(^\exists t \in \mathbb{R} \backslash \{0\})$ の同値類 $\mathrm{C}((1, 0))$.

[26)] この図を LaTeX で作図するのに 2 時間ほどかかった.

7.4　同値類であることの必要十分条件

命題 1

A に同値関係 $\sim$ が与えられているとする．このとき，次は同値 (必要十分条件).

(1) $a \sim b$.　　(2) $C(a) = C(b)$.　　(3) $C(a) \cap C(b) \neq \varnothing$.

証明：

(1)⇒(2)

$a \sim b$ とする.

$c \in C(b)$ とすると，$b \sim c$. 推移律より，$a \sim b$ かつ $b \sim c \Rightarrow a \sim c$. $\therefore c \in C(a)$. すなわち，$C(b) \subset C(a)$. …①

$d \in C(a)$ とすると，$a \sim d \Rightarrow d \sim a$. 推移律より，$d \sim a$ かつ $a \sim b \Rightarrow d \sim b \Rightarrow b \sim d$. $\therefore d \in C(b)$. すなわち，$C(a) \subset C(b)$. …②

したがって，①② より $C(a) = C(b)$.

(2)⇒(3)

$C(a) = C(b)$ とすると，$C(a) \cap C(b) = C(a) (= C(b)) \neq \varnothing$.

(3)⇒(1)

$C(a) \cap C(b) \neq \varnothing$ とする．このとき，$c \in C(a) \cap C(b)$ とすると，$a \sim c$ かつ $b \underset{③}{\sim} c$.

対称律より ③ は $c \sim b$. よって，推移律より，$a \sim c$ かつ $c \sim b \Rightarrow a \sim b$. ■

このことから，同値類の和集合 $= A$ であることがわかる. (重複なし.)

7.5　商集合

定義【商集合 (quotient set)】

集合 A 上に同値関係 $\sim$ が与えられているとする．また，その同値類を $C(a)$ とする．このとき，

$$A/_{\sim} := \{ C(a) \mid a \in A \}$$

を**商集合**という．(➡**注** “同値類 (集合)” を要素としている集合である.)

例 5

(1) $\mathbb{R}^2$ 上の同値関係 $(a, b) \sim (c, d) \overset{\text{def}}{\Longleftrightarrow} \sqrt{a^2+b^2} = \sqrt{c^2+d^2}$ を考える.

$C((0, 0)) = \{(0, 0)\}$, $C((a, b)) = \mathrm{C}_r := \left\{ (x, y) \in \mathbb{R}^2 \,\middle|\, \sqrt{x^2+y^2} = r \right\}$ と考えることができるので,

$\mathbb{R}^2/_{\sim} = \{ C(\mathrm{a}) \mid \mathrm{a} \in \mathbb{R}^2 \} = \{(0, 0)\} \cup \{ \mathrm{C}_r \mid r > 0 \}$

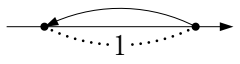
(2) $\mathbb{R}$ 上の同値関係 $a \sim b \overset{\text{def}}{\Longleftrightarrow} a - b \in \mathbb{Z}$ を考える.

$C(a) = \mathbb{Z} + a := \{ n + a \mid n \in \mathbb{Z} \}$ とかける. 例えば，$C(0) = \mathbb{Z} = C(100) = C(23) = C(n)$ $(n \in \mathbb{Z})$. $C(a) = C(b) \Leftrightarrow a - b \in \mathbb{Z}$ なので,

$0 \leqslant r < 1$ をつかって，$r = a - [a]$, $a = n + r$ $(n \in \mathbb{Z})$ と書くことにすると，$C(a) = C(r)$.

よって，$\mathbb{R}/_{\sim} = \{ C(a) \mid a \in \mathbb{R} \} = \{ \mathbb{Z} + r \mid 0 \leqslant r < 1 \}$. これを $\mathbb{R}/_{\sim} = \mathbb{R}/\mathbb{Z}$ ともかく.

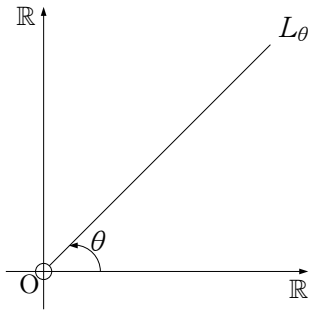
イメージ



(3) $\mathbb{R}^2 \backslash \{(0, 0)\}$ 上の同値関係 $(a, b) \sim (c, d) \overset{\text{def}}{\Longleftrightarrow} (c, d) = t(a, b)$ $(t > 0)$ を考える.

$L_\theta := \{ t(\cos\theta, \sin\theta) \mid t > 0 \}$ とすると，$\mathbb{R}^2 \backslash \{(0, 0)\}/_{\sim} = \{ L_\theta \mid 0 \leqslant \theta < 2\pi \}$.

イメージ



7.6　自然な射影

定義【自然な射影 (natural projection)】

集合 A 上に同値関係 $\sim$ が与えられているとする．このとき，写像 π を次のように定める．

$$\begin{array}{rccc} \pi & : & A & \longrightarrow & A/_{\sim} \\ & & a & \longmapsto & C(a) \end{array}$$

この写像 π のことを**自然な射影**または標準射影などという．(➡**注** この π は単なる記号であり，円周率とは関係ない.)
また，この写像は，A の任意の元 a をその a が属する同値類 $C(a)$ に対応させるので，π の値域は $A/_{\sim}$ となり，全射である．

7.7　写像のファイバー

定義【写像のファイバー】

写像 $f : A \ni a \mapsto b \in B$ に対して，f が全射になるような $a \in A$ 全体をなす集合を

$$\mathbf{f}^{-1}(b) := \{\, a \in A \,|\, b = f(a) \,\}$$

と表し，$\mathbf{f}^{-1}(b)$ を f の b 上のファイバーという.[27]　(➡**注** $\mathbf{f}^{-1}(b)$ は元ではなく，A の部分集合である.)

7.8　集合論的準同型定理

集合論的準同型定理

写像 $f : A \to B$ を全射であるとする．
(1) A 上の 2 項関係を $a \sim a' \iff f(a) = f(a')$ と定めると，$a \sim a'$ は同値関係である．
(2) $f(a) = b$ のとき，$C(a) = \mathbf{f}^{-1}(b)$.
(3) $A/_{\sim} = \left\{ \mathbf{f}^{-1}(b) \,|\, b \in B \right\}$.
(4) 自然な全単射 $\bar{f} : A/_{\sim} \to B$ が $\bar{f}\,(\mathbf{f}^{-1}(b)) = b$ により定まる．

<u>証明：</u>
(1) $a,\ a',\ a'' \in A$ を任意の元とする．
（ i ）$f(a) = f(a) \Leftrightarrow a \sim a$. よって反射律を満たす．
（ii ）$a \sim a' \Leftrightarrow f(a) = f(a') \Leftrightarrow f(a') = f(a) \Leftrightarrow a' \sim a$. $\therefore a \sim a' \Rightarrow a' \sim a$. よって対称律を満たす．
（iii）$a \sim a'$ かつ $a' \sim a''$ を仮定すると，$f(a) = f(a')$ かつ $f(a') = f(a'')$ である．$\therefore f(a) = f(a'') \Leftrightarrow a \sim a''$. 推移律を満たす．
よって，同値関係である．

(2) $C(a) = \{\, a' \in A \,|\, a \sim a' \,\} = \{\, a' \in A \,|\, f(a) = f(a') \,\} = \{\, a' \in A \,|\, b = f(a') \,\} = \mathbf{f}^{-1}(b)$.

(3) (2) より，$C(a) \in A/_{\sim}$ は $C(a) = \mathbf{f}^{-1}(b)$. 逆に，$b \in B$ に対して，$\mathbf{f}^{-1}(b) \neq \varnothing$ なので，$a \in \mathbf{f}^{-1}(b)$ をとるとき，$C(a) = \mathbf{f}^{-1}(b)$.
したがって，$A/_{\sim} \ni C(a) = \mathbf{f}^{-1}(b)$ なので，$A/_{\sim} = \{\, \mathbf{f}^{-1}(b) \,|\, b \in B \,\}$.

(4) (全射性)　$A/_{\sim}$ の任意の元 $\mathbf{f}^{-1}(b)$ を b に対応させているので，値域は B となり，全射である．
(単射性)　$\bar{f}(\mathbf{f}^{-1}(b)) = \bar{f}(\mathbf{f}^{-1}(b'))$ を仮定すると，$b = b'$. (2) より，$b = b' \Leftrightarrow b = f(a) = b' \Rightarrow \mathbf{f}^{-1}(b) = C(a) = \mathbf{f}^{-1}(b')$.
したがって，$\bar{f}(\mathbf{f}^{-1}(b)) = \bar{f}(\mathbf{f}^{-1}(b')) \Rightarrow \mathbf{f}^{-1}(b) = \mathbf{f}^{-1}(b')$ が示せたので，$\bar{f}$ は単射である．　■

[27] $\mathbf{f}^{-1}(b)$ という記号であり，逆写像という意味でないことに注意．誤解を招かないためにあえて $\mathbf{f}^{-1}(b)$ としたが一般的には $f^{-1}(b)$ や $f^{-1}(\{b\})$ と書かれている．

8　群・環

8.1　演算

定義【演算】

X を任意の集合とする．写像 f を次のように定める．

$$\begin{array}{rccc} f & : & X\times X & \longrightarrow & X \\ & & (x,\,y) & \longmapsto & f((x,\,y)) \end{array}$$

が与えられたとき，f を X 上の (2 項) **演算**という．$x*y := f((x,\,y))$ とかく．$(X,\,*)$: 演算を持つ集合.

例 1

$(\mathbb{Z},\,+)$, $(\mathbb{R},\,\cdot)$, $(\mathbb{R},\,+)$, ... など.

定義【結合律】

$(X,\,*)$: 演算を持つ集合とする．任意の $a,\,b,\,c\in X$ に対して，

$$(a*b)*c=a*(b*c)$$

が成り立つとき，$(X,\,*)$ は**結合律**を満たすという.

例 2

(1) $*=+$ なら，$(a+b)+c=a+(b+c)$.　　(2) $*=\cdot$ なら，$(a\cdot b)\cdot c=a\cdot(b\cdot c)$.

定義【可換】

$(X,\,*)$ が**可換** $\overset{\text{def}}{\Longleftrightarrow}$ 任意の $a,\,b\in X$ に対して，$a*b=b*a$ が成り立つ.

定義【単位元】

$(X,\,*)$ において，$e\in X$ が**単位元**であるとは，任意の $a\in X$ に対して，

$$a*e=e*a=a$$

が成り立つことをいう.

例 3

乗法なら $e=1$．加法なら $e=0$.

命題 1

単位元は存在するならば，唯一である.

証明：

$e,\,e'$ を単位元とすると，$e'=e'*e=e$. (1 つめの $=$ は e の単位元性，2 つめの $=$ は e' の単位元性.)　■

定義【逆元】

$(X,\,*)$ において，単位元 e が存在するとする．任意の $a\in X$ において，

$$a*a'=a'*a=e$$

が成り立つとき，a' は a の**逆元**であるという.

例 4

$\mathbb{R}$ 上の演算 $a*b=a+b-ab$ は結合律を満たす．また，単位元は 0 であり，$a\neq 1$ のときのみ逆元を持つ.

(結合律)

$a*(b*c)=a*(b+c-bc)=a+(b+c-bc)-a(b+c-bc)=a+b+c-bc-ab-ac+abc=(a+b-ab)+c-(a+b-ab)c=(a*b)*c$　■

(単位元)　$a*0=a+0-a\cdot 0=a,\ 0*a=0+a-0\cdot a=a$.　■

(逆元)　仮に a の逆元を a' とする．$a*a'=a+a'-aa'=0$ かつ $a'*a=a'+a-a'a=0$ が成り立つ条件を調べればよい.

$a+a'-aa'=0\Leftrightarrow a'(1-a)=-a\Leftrightarrow a'=\dfrac{a}{a-1}$．よって a が逆元を持つための条件は $a\neq 1$．またその時の a の逆元は $\dfrac{a}{a-1}$.

8.2　モノイド

定義【モノイド (monoid)】

$(X, *)$ が結合律を満たし，単位元を持つとき，**モノイド**であるという．

命題 2

モノイドにおいて，元 a の逆元が存在すれば唯一である．

証明：
a', a'' を a の逆元であるとする．
$a' = a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''$　$\therefore a' = a''$. ■

8.3　群

定義【群 (group)】

モノイド $(X, *)$ において，任意の $a \in X$ に逆元が存在するとき，$(X, *)$ は**群**であるという．

例 5

(1) $(\mathbb{Z}, +)$ は (可換) 群である．

∵

任意の $a, b, c \in \mathbb{Z}$ に対して，(結合律) $a + (b + c) = (a + b) + c$. (単位元) $a + 0 = 0 + a = a$. (逆元) $a + (-a) = (-a) + a = 0$. ■

$(\mathbb{Q}, +), (\mathbb{R}, +)$ も同様に群である．

(2) $(\mathbb{Q}\backslash\{0\}, \cdot)$ は群である．しかし $(\mathbb{Q}, \cdot)$ は群ではない．モノイドである．

8.4　加法群

定義【加法群 (additive group)】

集合 M 上に演算 $(a, b) \mapsto a + b$ があり，

- **結合律**「$(a + b) + c = a + (b + c)$.」
- **単位元 (零元)**「$0 \in M$ があり，任意の $a \in M$ に対して，$a + 0 = 0 + a = a$.」
- **逆元**「任意の $a \in M$ に対して，$a + (-a) = (-a) + a = 0$ なる $-a \in M$ が存在.」
- **可換性**「任意の $a, b \in M$ に対して，$a + b = b + a$.」

の 4 つが成り立つとき，M を**加法群**という．

定義【部分加法群】

M を加法群とする．M の空でない部分集合 N に対して，

- $a, b \in N \Rightarrow a + b \in N$　　- $a \in N \Rightarrow -a \in N$

が成り立つとき，N は M の**部分加法群**という．[28] (➡**注** $0 \in N$ である．$\because a \in N \Rightarrow -a \in N, N \ni a + (-a) = 0$.)

例 6

(1) $M = \mathbb{R}, N = \mathbb{Z}$ のとき，N は M の部分加法群である．　　(2) $M = \mathbb{R}, N = \mathbb{Q}$ のとき，N は M の部分加法群である．

(3) $M = \mathbb{Z}, N = n\mathbb{Z} := \{na \mid a \in \mathbb{Z}\}$ のとき，N は M の部分加法群である．

定義

M を加法群とする．任意の $a, b \in M$ に対して，

$$a + (-b) \overset{\text{def}}{\Longleftrightarrow} a - b$$

例 7　$-(a - b) = b - a$ を示す．$(a - b) + (b - a) = 0$ を示せば，逆元の一意性より，$-(a - b) = b - a$ である．

$(a - b) + (b - a) = (a + (-b)) + (b + (-a)) = (a + (-b) + b) + (-a) = (a + (-b + b)) + (-a) = a + (-a) = 0$.

[28] N が部分加法群であることの必要十分条件は，• $N \neq \varnothing (0 \in N)$. • $a, b \in N \Rightarrow a + b \in N$. • $c \in N \Rightarrow -c \in N$. が成り立つことである．

8.5　剰余加法群

命題３

M：加法群，N：M の部分加法群とする．このとき，M 上の２項関係を

$$a \sim b \Longleftrightarrow a-b \in N$$

と定める．これは M 上の同値関係である．

証明：
任意の $a, b, c \in M$ に対して，
$a-a=0$．N は部分加法群なので $0 \in N$．よって $a-a \in N \Leftrightarrow a \sim a$ である．よって**反射律**を満たす．…(i)
$a \sim b$ と仮定すると，$a-b \in N$．N は部分加法群より $-(a-b) \in N$．
8.4 の例７より，$-(a-b)=b-a \in N \Leftrightarrow b \sim a$．よって $a \sim b \Rightarrow b \sim a$ より**対称律**を満たす．…(ii)
$a \sim b$ かつ $b \sim c$ を仮定すると，$a-b \in N$ かつ $b-c \in N$ である．N は部分加法群であるから，$(a-b)+(b-c) \in N$．
M は加法群なので (可換性と) 結合律より，$(a-b)+(b-c)=a+((-b)+b)+(-c)=a-c \in N \Leftrightarrow a \sim c$．
よって $a \sim b$ かつ $b \sim c \Rightarrow a \sim c$ であるから**推移律**を満たす．…(iii) したがって (i)(ii)(iii) より M 上の同値関係である．　■

定義【剰余加法群】

M：加法群，N：M の部分加法群とする．
$a \sim b \Longleftrightarrow a-b \in N$ により定まる M 上の同値関係の商集合 $M/_\sim$ を M/N と表し，この M/N を**剰余加法群**という．[29)]

8.6　剰余加法群 M/N 上の演算“$+$”

定義【M/N 上の演算 $+$】

M：加法群，N：M の部分加法群とするとき，剰余加法群 M/N 上の演算を次のように定める．[30)]

(b)　$$(C(a), C(b)) \longmapsto C(a+b) =: C(a)+C(b)$$

例８
$M=\mathbb{Z}$, $N=5\mathbb{Z}$ の場合：
$\mathbb{Z}/5\mathbb{Z}$．つまり mod 5 の世界での話では，$(C(-1), C(12)) \mapsto C(-1+12)=C(11)=C(1)$ となる．
$C(-1)=C(4)$, $C(12)=C(2) \Rightarrow C(4+2)=C(6)=C(1)=C(11)=C(-1+12)=C(-1)+C(12)$ となっている．

定理１

M/N 上の演算 (b) により，M/N は加法群の構造をもつ．

証明：
- **結合律**

$(C(a)+C(b))+C(c)=C(a+b)+C(c)=C((a+b)+c)=C(a+(b+c))=C(a)+C(b+c)+C(a)+(C(b)+C(c))$.
- **可換性**

$C(a)+C(b)=C(a+b)=C(b+a)=C(b)+C(a)$.
- **単位元**

$C(0)$ が単位元である．$C(a)+C(0)=C(a+0)=C(a)$, $C(0)+C(a)=C(0+a)=C(a)$.
- **逆元**

$C(-a)$ が逆元である．$C(a)+C(-a)=C(a+(-a))=C(0)$, $C(-a)+C(a)=C(-a+a)=C(0)$.　■

[29)] また，同値類のことを**剰余類**という．(剰余類の定義が *6.1* にあったがこちらのの方がより一般化された定義である．)

[30)] **問**．これはちゃんと定義になっているのか？ (well-defined なのか？) Answer: なっている．
$\because C(a)=C(a')$, $C(b)=C(b') \Rightarrow C(a+b)=C(a'+b')$ を示せばよい．
$C(a)=C(a')$ が成り立つのは *7.4* の命題１より，$a \sim a'$ のとき，つまり $a-a' \in N$．同様にして $C(b)=C(b')$ が成り立つのは $b \sim b' \Leftrightarrow b-b' \in N$ のときである．
N は (部分) 加法群より $(a-a')+(b-b') \in N$ である．$a+b-(a'+b')=a+b+(-b'-a')=(a-a')+(b-b') \in N$．$\therefore (a+b)-(a'+b') \in N$．よって well-defined．　■

8.7　準同型写像

定義【準同型写像】

M, N を加法群とする．写像 $f : M \to N$ が加法群の**準同型**写像であるとは，任意の $a, b \in M$ に対し，

- $f(0) = 0$
- $f(a+b) = f(a) + f(b)$

が成り立つことをいう．単に準同型であるともいう．さらに，f が全単射のとき，f は**同型**であるという．

例 9

自然な射影 $\pi : M \ni a \mapsto C(a) \in M/N$ は準同型である．

Check! (1) $\pi(0) = C(0) = 0$. (2) $\pi(a+b) = C(a+b) = C(a) + C(b) = \pi(a) + \pi(b)$.

命題 4

$f : M \to N$ を加法群の準同型写像であるとする．このとき，次が成り立つ．

(1) $f(-a) = -f(a)$　　(2) $f(a-b) = f(a) - f(b)$

証明：

(1) $f(-a) + f(a) = 0$ を示せばよい．

$f(-a) + f(a) = f(-a+a) = f(0) = 0$. 逆元の一意性より，$-f(a) = f(-a)$.

(2) (1) より，$f(a-b) = f(a+(-b)) = f(a) + f(-b) = f(a) - f(b)$. ■

命題 5

M, N：加法群，$f : M \to N$ を準同型写像とする．このとき，

$$\mathrm{Ker}(f) := \{ a \in M \mid f(a) = 0 \},\ \mathrm{Im}(f) := \{ n \in N \mid {}^{\exists}a \in M \text{ s.t. } f(a) = n \}$$

と定めると，$\mathrm{Ker}(f)$ は M の部分加法群，$\mathrm{Im}(f)$ は N の部分加法群である．

証明：

$\mathrm{Ker}(f)$ が M の部分加法群であることを示す

f は準同型より，$f(0) = 0$ なので $0 \in \mathrm{Ker}(f)$. $\therefore \mathrm{Ker}(f) \neq \varnothing$. …❶

任意に $x, y \in \mathrm{Ker}(f)$ とすると，$f(x) = 0$, $f(y) = 0$. いま，$\mathrm{Ker}(f)$ の定義より $x, y \in M$ である．

M は加法群より，$-x \in M$, $x + y \in M$. 命題 4 より $f(-x) = -f(x) = -0 = (-0) + 0 = 0$. $\therefore -x \in \mathrm{Ker}(f)$.

よって $x \in \mathrm{Ker}(f) \Rightarrow -x \in \mathrm{Ker}(f)$. …❷

また，f は準同型より $f(x+y) = f(x) + f(y)$ なので，$f(x+y) = f(x) + f(y) = 0 + 0 = 0$. $\therefore x + y \in \mathrm{Ker}(f)$.

よって $x, y \in \mathrm{Ker}(f) \Rightarrow x + y \in \mathrm{Ker}(f)$. …❸

$\mathrm{Im}(f)$ が N の部分加法群であることを示す

M は加法群より $0 \in M$. f は準同型より $0 = f(0) \in \mathrm{Im}(f)$. $\therefore \mathrm{Im}(f) \neq \varnothing$. …❹

任意に $\xi, \eta \in \mathrm{Im}(f)$ とすると，${}^{\exists}a, {}^{\exists}b \in M$ s.t. $f(a) = \xi$, $f(b) = \eta$ である．

M は加法群より $-a \in M$, $a + b \in M$. 命題 4 より $-\xi = -f(a) = f(-a) \in \mathrm{Im}(f)$. よって $\xi \in \mathrm{Im}(f) \Rightarrow -\xi \in \mathrm{Im}(f)$. …❺

f が準同型より，$f(a) + f(b) = f(a+b)$. $\xi + \eta = f(a) + f(b) = f(a+b) \in \mathrm{Im}(f)$. よって $\xi, \eta \in \mathrm{Im}(f) \Rightarrow \xi + \eta \in \mathrm{Im}(f)$. …❻

❶❷❸ より $\mathrm{Ker}(f)$ は M の部分加法群である．

❹❺❻ より $\mathrm{Im}(f)$ は N の部分加法群である． ■

8.8　準同型定理

準同型定理

M, N：加法群，$f : M \to N$ を加法群の準同型写像とする．このとき，自然な同型写像

$$\begin{array}{ccccc} \bar{f} & : & M/\mathrm{Ker}(f) & \longrightarrow & \mathrm{Im}(f) \\ & & C(a) & \longmapsto & f(a) \end{array}$$

が存在する．

証明：

$\bar{f}$ が well-defined であること ($C(a) = C(a') \Rightarrow f(a) = f(a')$) を示す．

$$\begin{aligned} C(a) = C(a') \iff a \sim a' &\iff a - a' \in \mathrm{Ker}(f) \\ &\iff f(a - a') = 0 \\ &\iff f(a) - f(a') = 0 \\ &\iff f(a) = f(a') \end{aligned}$$

よって well-defined.

また，これを逆にたどっていくと，$f(a) = f(a') \Leftrightarrow \bar{f}(C(a)) = \bar{f}(C(a')) \Rightarrow C(a) = C(a')$ である．つまり $\bar{f}$ は単射である．

さらに，同値類 $C(a)$ を $f(a)$ に対応させているので，$\bar{f}$ の値域は $\mathrm{Im}(f)$ である．よって，$\bar{f}$ は全射である．

次に，$\bar{f}$ が準同型であることを示す．

（ i ）$\bar{f}(C(0)) = f(0) = 0$.　（ ii ）$\bar{f}(C(a) + C(b)) = \bar{f}(C(a+b)) = f(a+b) = f(a) + f(b) = \bar{f}(C(a)) + \bar{f}(C(b))$.

よって，$\bar{f}$ は準同型である．

したがって，$\bar{f}$ は全単射かつ準同型であるから，同型写像である．　■

8.9　環

定義【環 (ring)】

集合 R 上に，加法 $+$，乗法 $\cdot$ と呼ばれる 2 つの演算が定義されており，

加法に関しては加法群 (単位元は 0_R)，乗法に関してはモノイド (単位元は 1_R) であって，

分配律　$(a+b)\cdot c = a\cdot c + b\cdot c, \quad a\cdot(b+c) = a\cdot b + a\cdot c$

が成り立つとき，R は**環**であるという．さらに，乗法に関して可換であるとき，**可換環** (commutative ring) という．[31)]

命題 6

R を環とする．次が成り立つ．

(1) 任意の $a \in R$ に対して，$0\cdot a = a\cdot 0 = 0$.　　(2) 任意の $a, b \in R$ に対して，$(-a)\cdot b = a\cdot(-b) = -(a\cdot b)$.

証明：

(1) $0\cdot a = (0+0)\cdot a = 0\cdot a + 0\cdot a$.　$\therefore 0\cdot a = 0$.　　$a\cdot 0 = a\cdot(0+0) = a\cdot 0 + a\cdot 0$.　$\therefore a\cdot 0 = 0$. [32)]

(2) $(-a)\cdot b + a\cdot b = (-a+a)\cdot b = 0\cdot b = 0$. $\therefore -(a\cdot b) = (-a)\cdot b$.

$a\cdot(-b) + a\cdot b = a\cdot(-b+b) = a\cdot 0 = 0$. $\therefore -(a\cdot b) = a\cdot(-b)$.　■

例 10

(1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ は可換環である．

(2) $R = \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ とするとき，R を成分にもつ n 次正方行列全体の集合 $M_n(R)$ は環である．[33)]

このとき，加法に対する単位元は零行列 O，乗法に対する単位元は単位行列 E_n である．➪**注**　今後，$a\cdot b$ などを略して，ab などとかくことがある．

[31)] 可換環 K において，0 を除いた集合 $K\backslash\{0\}$ が群をなすとき，K は可換体 (commutative field) であるという．例えば $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

[32)] $a + x = a \Rightarrow x = 0$ より．($\because x = x + 0 = x + \big(a + (-a)\big) = (x + a) + (-a) = a + (-a) = 0$.)

[33)] $M_n(R) := \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \middle| \, a_{11}, \ldots, a_{nn} \in R \right\}$.

8.10　環準同型写像

定義【環準同型】

R, R' を環とする．写像 $f : R \to R'$ が**環準同型**であるとは
(1) $f(1_R) = 1_{R'}$　　(2) $f(a+b) = f(a) + f(b)$　$(a, b \in R)$　　(3) $f(a \cdot b) = f(a) \cdot f(b)$　$(a, b \in R)$
が成り立つことをいう．さらに，f が全単射であるとき f は**環同型**であるという．

命題 7

$f : R \to R'$ を環準同型とする．次が成り立つ．
(i) $f(0_R) = 0_{R'}$　　(ii) $f(-a) = -f(a)$　　(iii) $f(a-b) = f(a) - f(b)$　$(a, b \in R)$

証明：
(i) 定義の (1),(2) より，$1 = f(1) = f(1+0) = f(1) + f(0) = 1 + f(0)$．$\therefore f(0) = 0$.
(ii),(iii) は加法群の準同型のときと同じ．　■

命題 8

$f : R \to R'$ を環準同型とする．このとき次が成り立つ．
(1) $x, y \in \mathrm{Ker}(f) \Longrightarrow x + y \in \mathrm{Ker}(f)$.　　(2) $x \in \mathrm{Ker}(f)$, $a \in R \Rightarrow ax \in \mathrm{Ker}(f)$, $xa \in \mathrm{Ker}(f)$.

証明：
(1) $x, y \in \mathrm{Ker}(f)$ とすると $f(x) = 0$, $f(y) = 0$.
f は環準同型より，$f(x+y) = f(x) + f(y) = 0 + 0 = 0$．$\therefore x + y \in \mathrm{Ker}(f)$.
(2) $x \in \mathrm{Ker}(f)$, $a \in R$ とすると，
f は環準同型より，$f(a \cdot x) = f(a) \cdot f(x) = f(a) \cdot 0_{R'} = 0_{R'}$．$\therefore ax \in \mathrm{Ker}(f)$.
同様に $f(xa) = f(x) \cdot f(a) = 0_{R'} f(a) = 0_{R'}$ なので $xa \in \mathrm{Ker}(f)$.　■

➡**注** (2) の主張はあくまで，ax, xa が $\mathrm{Ker}(f)$ の元であるということであって，$ax = xa$ とは言ってない!!!

8.11　イデアル

定義【イデアル (ideal)】

環 R の空でない部分集合 I が
(1) $x, y \in I \Longrightarrow x + y \in I$.　　(2) $x \in I$, $a \in R \Rightarrow ax \in I$, $xa \in I$. を満たすとき，I は R の**両側イデアル**であるという．また，
(2L) $x \in I$, $a \in R \Longrightarrow ax \in I$.　　(2R) $x \in I$, $a \in R \Longrightarrow xa \in I$.
とするとき，(1) と (2L) を満たすとき I は**左イデアル**，(1) と (2R) を満たすとき I は**右イデアル**という．R が可換環の場合は，単に**イデアル**という．

命題 8 の主張より「環準同型の核空間は両側イデアルである」といえる．任意の環 R において $\{0_R\}$ および R 自身は R の両側イデアルである．

例 11

(1) n を整数としたとき，$I = n\mathbb{Z} := \{na \mid a \in \mathbb{Z}\}$ は $\mathbb{Z}$ のイデアルである．

(2) R を可換環とする．このとき，$M_2(R)$ の部分集合 $I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \in M_2(R) \,\middle|\, a, b \in R \right\}$ は $M_2(R)$ の左イデアルである．

$\because$ 任意の行列 $A = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$, $B = \begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix} \in I$ に対して，$A + B = \begin{pmatrix} a+c & 0 \\ b+d & 0 \end{pmatrix} \in I$.

任意の行列 $X = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in M_2(R)$, $A = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \in I$ に対して，$XA = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} xa+yb & 0 \\ za+wb & 0 \end{pmatrix} \in I$.

よって左イデアルである．　■

8.12　剰余加法群 R/I 上の演算 “$\cdot$”

定理 2

R を環，I を R の両側イデアルとする．剰余加法群 R/I 上の演算 (乗法)

(ｔ)　　$C(a)\cdot C(b)=C(a\cdot b)$

が定義できる．この演算 (ｔ) および加法 (ｂ) により，R/I は環の構造を持つ．

証明：

（ i ）well-defined であることを示す．つまり，$C(a)=C(a'),\ C(b)=C(b')\Longrightarrow C(a\cdot b)=C(a'\cdot b')$ を示す．

$C(a)=C(a')$ が成り立つのは $a\sim a'$ のとき，$a\sim a'\Leftrightarrow a-a'\in I$．同様に，$C(b)=C(b')\Leftrightarrow b\sim b'\Leftrightarrow b-b'\in I$．

$$\begin{aligned} ab-a'b' &= ab-a'b'+0\\ &= ab-a'b'+a'b+(-a'b)\\ &= ab-a'b+a'b-a'b'\\ &= (a+(-a'))b+a'(b+(-b')) \end{aligned}$$

I はイデアルより $(a-a')b\in I,\ a'(b-b')\in I,\ I\ni(a-a')b+a'(b-b')=ab-a'b'\Leftrightarrow ab\sim a'b'\Leftrightarrow C(a\cdot b)=C(a'\cdot b')$.

$\therefore C(a\cdot b)=C(a'\cdot b')$．よって well-defined.

（ ii ）乗法の結合律を示す．

$$\begin{aligned} C(a)\cdot(C(b)\cdot C(c)) &= C(a)\cdot C(b\cdot c)\\ &= C(a\cdot(b\cdot c))\\ &= C((a\cdot b)\cdot c)\\ &= C(a\cdot b)\cdot C(c)\\ &= (C(a)\cdot C(b))\cdot C(c). \end{aligned}$$

（iii）$C(1_R)$ が乗法の単位元であることを示す．

$C(1_R)\cdot C(a)=C(1_R\cdot a)=C(a),\ C(a)\cdot C(1_R)=C(a\cdot 1_R)=C(a)$.

（iv）分配律を示す．

$C(a)\cdot(C(b)+C(c))=C(a)\cdot C(b+c)=C(a\cdot(b+c))=C(ab+ac)=C(a\cdot b)+C(a\cdot c)=C(a)\cdot C(b)+C(a)\cdot C(c)$.

逆も同様にして，

$(C(a)+C(b))\cdot C(c)=C(a+b)\cdot C(c)=C((a+b)\cdot c)=C(ac+bc)=C(a\cdot c)+C(b\cdot c)=C(a)\cdot C(c)+C(b)\cdot C(c)$. ■

この定理によって得られる環 R/I を**剰余環**という．

8.13　部分環

定義【部分環】

環 R の部分加法群 S が

(1) $1_R\in S$.　　(2) $a,b\in S\Longrightarrow ab\in S$. を満たすとき，$S$ は R の**部分環**であるという．

命題 9

R,R'：環，$f:R\to R'$ を環準同型写像とする．このとき，次が成り立つ．　(1) $\mathrm{Im}(f)$ は R' の部分環.　(2) $\mathrm{Ker}(f)$ は R の両側イデアル.

証明：

(1) $\alpha,\beta\in\mathrm{Im}(f)$ とすると，$^{\exists}\xi,\eta\in R$ s.t. $f(\xi)=\alpha,\ f(\eta)=\beta$. f は環準同型より，

$-\alpha=-f(\xi)=f(-\xi)\in\mathrm{Im}(f),\ \alpha+\beta=f(\xi)+f(\eta)=f(\xi+\eta)\in\mathrm{Im}(f)$．よって $\mathrm{Im}(f)$ は R' の部分加法群である．　…①

$1_{R'}\in R'$ とする．f は環準同型なので $1_{R'}=f(1_R)\in\mathrm{Im}(f)$.　…②

$x,y\in\mathrm{Im}(f)$ とすると，$^{\exists}a,b\in R$ s.t. $f(a)=x,\ f(b)=y$ である．f は環準同型より $xy=f(a)\cdot f(b)=f(a\cdot b)\in\mathrm{Im}(f)$.　…③

①②③ より $\mathrm{Im}(f)$ は R' の部分環である．

(2) *8.10* の命題 8 より．■

8.14　環準同型定理

環準同型定理

R, R' を環，$f : R \to R'$ を環準同型とする．このとき，自然な環同型写像

$$\begin{array}{rccc} \bar{f} & : & R/\mathrm{Ker}(f) & \longrightarrow & \mathrm{Im}(f) \\ & & C(a) & \longmapsto & f(a) \end{array}$$

が存在する．

証明：

$\bar{f}$ が環同型であることを示す．

(i) $\bar{f}(C(a)\cdot C(b)) = \bar{f}(C(a\cdot b)) = f(a\cdot b) = f(a)\cdot f(b) = \bar{f}(C(a))\cdot\bar{f}(C(b))$.

(ii) $\bar{f}(C(1_R))\cdot\bar{f}(C(a)) = f(1_R)\cdot f(a) = f(1_R\cdot a) = f(a) = \bar{f}(C(a))$.

$\bar{f}(C(a))\cdot\bar{f}(C(1_R)) = f(a)\cdot f(1_R) = f(a\cdot 1_R) = f(a) = \bar{f}(C(a))$.

よって，(i),(ii) より $\bar{f}$ は環準同型である．

<単射性>

$\bar{f}(C(a)) = \bar{f}(C(a')) \Rightarrow f(a) = f(a') \Leftrightarrow f(a) - f(a') = 0 \Leftrightarrow f(a-a') = 0 \Leftrightarrow a - a' \in \mathrm{Ker}(f) \Leftrightarrow a \sim a' \Leftrightarrow C(a) = C(a')$.

<全射性>

同値類 $C(a)$ を $f(a)$ に対応させているので，$\bar{f}$ の値域は $\mathrm{Im}(f)$ となるので，全射． ■

付録 A　環準同型定理の例

A.1　環の例

A.1.1　多項式環

R：可換環とする．このとき，

$$a_n x^n + \cdots + a_1 x + a_0 \qquad (a_0, a_1, \ldots, a_n \in R)$$

を $\boldsymbol{R}$ **係数の多項式**という．また，R 係数の多項式全体の集合を

$$R[x]$$

により表す.[34] $R[x]$ は**可換環**になる．単位元は 1 であり，零元は 0.

A.2　イデアルの作り方

R：可換環とする．$a \in R$ をひとつとる．$I := \{xa \mid x \in R\}$ とすると，I はイデアルである．
$\because$
(1) $xa, ya \in I$ を任意の元とする．このとき，$xa + ya = (x+y)a \in I$.
(2) $xa \in I$, $b \in R$ を任意にとると，$b(xa) = (bx)a \in I$, $(xa)b = x(ab) = (xb)a \in I$. ■

このような $I = \{xa \mid x \in R\}$ の成分を a の**倍元**といい，$I = (a)$ と表す.

もっと一般に，$a_1, a_2, \ldots, a_n \in R$ をとり，$I = \{x_1a_1 + x_2a_2 + \cdots + x_na_n \mid x_1, x_2, \ldots, x_n \in R\}$ とすると，I は R のイデアルである．
これを $a_1, a_2, \ldots, a_n$ が**生成するイデアル**といい，

$$I = (a_1, a_2, \cdots, a_n)$$

とかく. (環論の話をしているときは．ベクトルではない.)

A.3　環準同型の例

$\phi(x) := a_n x^n + \cdots + a_1 x + a_0$, i：虚数単位とする．写像 f を次のように定める．

$$\begin{array}{rccc} f & : & \mathbb{R}[x] & \longrightarrow & \mathbb{C} \\ & & \phi(x) & \longmapsto & \phi(i) \end{array}$$

つまり，$f(\phi(x)) = \phi(i)$．このとき，f は環準同型である．
$\because$
(1) $f(1_{\mathbb{R}[x]}) = 1_{\mathbb{C}}$.　　(2) $f(\phi(x) + \phi(x)) = \phi(i) + \phi(i) = f(\phi(x)) + f(\phi(x))$.　　(3) $f(\phi(x)\phi(x)) = \phi(i)\phi(i) = f(\phi(x))f(\phi(y))$.
$\mathrm{Im}(f) = \mathbb{C}$ は明らか.
$\mathrm{Ker}(f) = (x^2+1) = \{\phi(x)(x^2+1) \mid \phi(x) \in \mathbb{R}[x]\}$ である．$\because f(\phi(x)(x^2+1)) = \phi(i)(i^2+1) = \phi(i)(-1+1) = 0$　$\therefore \phi(x)(x^2+1) \in \mathrm{Ker}(f)$.
$g(x) \in \mathrm{Ker}(f)$ とする．$g(x) = q(x)(x^2+1) + ax + b$ とかける．$(a, b \in \mathbb{R})$
$0 = f(g(x)) = g(i) = q(i)(i^2+1) + ai + b = ai + b$．これは $a = 0 = b$ を意味する．したがって，$g(x) = q(x)(x^2+1)$.
よって，**環同型写像** $\bar{f}$ を次のように作れる．

$$\begin{array}{rccc} \bar{f} & : & \mathbb{R}[x]/_{(x^2+1)} & \longrightarrow & \mathbb{C} \\ & & C(x) & \longmapsto & i \end{array}$$

補足：$\mathbb{R}[x]/_{(x^2+1)}$ は $x^2 \equiv -1 \pmod{x^2+1}$ を意味している.

この他にも，例えば，$\sqrt{2}$ を作り出したいのなら，$\mathbb{Q}[x]/_{(x^2-2)} \to \mathbb{R}$ 等とすればよい.

参考文献

[1] 中島 匠一　（2017）『共立講座　21 世紀の数学 ⑨　代数と数論の基礎』　共立出版株式会社

[2] 内田 伏一　（2018）『数学シリーズ　集合と位相』　裳華房

[34] [] であることに注意．() だと，また意味が変わってくる．