• 法 m に関する剰余類

$$\begin{aligned} a+m\mathbb{Z} &= \{a+mn \,|\, n\in\mathbb{Z}\} \\ &= \{\ldots, a-2m,\, a-m,\, a,\, a+m,\, a+2m, \ldots\} \\ &= [a] = \overline{a} \end{aligned}$$

m 個 $(a=0,\ldots,m-1)$ からなる集合 (← これは，同値関係 $\equiv$ による $\mathbb{Z}$ の商集合 $\mathbb{Z}/\equiv$ であった)

$$\begin{aligned} \mathbb{Z}/m\mathbb{Z} &= \{m\mathbb{Z}, 1+m\mathbb{Z}, 2+m\mathbb{Z}, \ldots, (m-1)+m\mathbb{Z}\} \\ &= \{[0],[1],[2],\ldots,[m-1]\} \\ &= \{\overline{0},\overline{1},\overline{2},\ldots,\overline{m-1}\} \end{aligned}$$

を考える．ここで，$a+m\mathbb{Z}=\{a+mn\,|\,n\in\mathbb{Z}\}=[a]=\overline{a}$ であることに注意する．

• $a+\mathbb{Z}$ は無限集合であり，$a+\mathbb{Z}=[a]=\overline{a}$ の**代表元** a **の取り方は無限**にある．たとえば，$m=5$ のとき，$[-7]=[-2]=[3]=[8]=[3+5n]$ となっている．より詳しくは，次が成り立つ．

命題 [1]. 次の (1)–(5) は同値である．
(1) $a+m\mathbb{Z}=b+m\mathbb{Z}$, (2) $-a+b\in m\mathbb{Z}$, (3) $b\in a+m\mathbb{Z}$, (4) $a\in b+m\mathbb{Z}$, (5) $(a+m\mathbb{Z})\cap(b+m\mathbb{Z})\neq\emptyset$.

☉ (1)$\Longrightarrow$(2) $b\in b+m\mathbb{Z}=a+m\mathbb{Z}$ より $\exists n\in\mathbb{Z}$ s.t. $b=a+mn$. よって，$-a+b=mn\in m\mathbb{Z}$.
(2)$\Longrightarrow$(3) $\exists n\in\mathbb{Z}$ s.t. $-a+b=mn$ より，$b=a+mn\in a+m\mathbb{Z}$,
(3)$\Longrightarrow$(4) $\exists n\in\mathbb{Z}$ s.t. $b=a+mn$ より，$a=b-mn=b+m(-n)\in m\mathbb{Z}$,
(4)$\Longrightarrow$(5) $a\in b+m\mathbb{Z}$ かつ $b\in b+m\mathbb{Z}$ より，$(a+m\mathbb{Z})\cap(b+m\mathbb{Z})\neq\emptyset$,
(5)$\Longrightarrow$(1) $\exists c\in(a+m\mathbb{Z})\cap(b+m\mathbb{Z})$ に対して，$\exists n_1,n_2\in\mathbb{Z}$ s.t. $c=a+mn_1=b+mn_2$．よって，$a=b+m(n_2-n_1)$．いま，$\forall a+mn\in a+m\mathbb{Z}$ に対して，$a+mn=b+m(n_2-n_1+n)\in b+\mathbb{Z}$ であるから，$a+m\mathbb{Z}\subset b+m\mathbb{Z}$．$a$ と b を入れ換えれば，$b+m\mathbb{Z}\subset a+m\mathbb{Z}$ となり，$a+m\mathbb{Z}=b+m\mathbb{Z}$.

• $(a+m\mathbb{Z})=[a]=\overline{a}$ より，上の (1)–(5) は次のように書いても同じことである：
(1) $[a]=[b]$, (2) $-a+b\in m\mathbb{Z}$, (3) $b\in[a]$, (4) $a\in[b]$, (5) $[a]\cap[b]\neq\emptyset$.
(1) $\overline{a}=\overline{b}$, (2) $-a+b\in m\mathbb{Z}$, (3) $b\in\overline{a}$, (4) $a\in\overline{b}$, (5) $\overline{a}\cap\overline{b}\neq\emptyset$.

• $\#(a+m\mathbb{Z})=\#[a]=\#\overline{a}=\infty$ ではあるが，$\#(\mathbb{Z}/m\mathbb{Z})=m$ なので，集合 $\mathbb{Z}/m\mathbb{Z}=\{\overline{0},\ldots,\overline{m-1}\}$ に2つの演算，**加法** $+$ **と乗法** $\cdot$ **を (感覚と一致するように) 以下の演算表により定義できる**：

$(\mathbb{Z}/m\mathbb{Z},+)$ の演算表． (← 単位元 $\overline{0}$ で，群になっている?)

$m=2$

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

$m=3$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$m=4$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$m=5$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$m=6$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$(\mathbb{Z}/m\mathbb{Z},\cdot\,)$ の演算表． (← $\overline{1}$ は単位元?，群にはならない?，半群?)

$m=2$

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

$m=3$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

$m=4$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$m=5$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$m=6$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$m=7$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{1}$	$\overline{3}$	$\overline{5}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{1}$	$\overline{4}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{1}$	$\overline{5}$	$\overline{2}$	$\overline{6}$	$\overline{3}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$m=8$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{1}$	$\overline{4}$	$\overline{7}$	$\overline{2}$	$\overline{5}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{2}$	$\overline{7}$	$\overline{4}$	$\overline{1}$	$\overline{6}$	$\overline{3}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$m=9$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{0}$	$\overline{3}$	$\overline{6}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{3}$	$\overline{7}$	$\overline{2}$	$\overline{6}$	$\overline{1}$	$\overline{5}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{1}$	$\overline{6}$	$\overline{2}$	$\overline{7}$	$\overline{3}$	$\overline{8}$	$\overline{4}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{3}$	$\overline{0}$	$\overline{6}$	$\overline{3}$	$\overline{0}$	$\overline{6}$	$\overline{3}$
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{8}$	$\overline{0}$	$\overline{8}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

一般の $m\in\mathbb{N}$ に対しても，集合 $\mathbb{Z}/m\mathbb{Z}=\{\overline{0},\dots,\overline{m-1}\}$ に加法 $+$ と乗法 $\cdot$ を定義したい！
しかし，いちいち演算表を書いていたのでは，非常に大変である．($\leftarrow$ 特に乗法 $\cdot$ について)

$\downarrow$どうするか

一般に，a を代表元とする剰余類 (同値類) $\overline{a}=[a]$ と b を代表元とする剰余類 $\overline{b}=[b]$ の和を，整数 a と b の和 $a+b$ が属する類 $\overline{a+b}=[a+b]$, 剰余類 $\overline{a}=[a]$ と剰余類 $\overline{b}=[b]$ の積を積 ab が属する類 $\overline{ab}=[ab]$ と定めればよい.

定義 ($\mathbb{Z}/m\mathbb{Z}$ 上の加法と乗法)． 集合 $\mathbb{Z}/m\mathbb{Z}=\{[0],\dots,[m-1]\}=\{\overline{0},\dots,\overline{m-1}\}$ 上の加法 $[a]+[b]$ $(\overline{a}+\overline{b})$ と乗法 $[a]\cdot[b]$ $(\overline{a}\cdot\overline{b})$ を以下のように定める:

$$(a+m\mathbb{Z})+(b+m\mathbb{Z}):=(a+b)+m\mathbb{Z},\qquad [a]+[b]:=[a+b],\qquad \overline{a}+\overline{b}:=\overline{a+b},$$
$$(a+m\mathbb{Z})\cdot(b+m\mathbb{Z}):=(a\cdot b)+m\mathbb{Z},\qquad [a]\cdot[b]:=[a\cdot b],\qquad \overline{a}\cdot\overline{b}:=\overline{a\cdot b}.$$

しかし，ここで問題が発生する. $a+m\mathbb{Z}$ 及び $b+m\mathbb{Z}$ の代表元は a,b 以外にもそれぞれ無限に選び方がある．それにも関わらず，勝手に取った代表元 a, b の和 $a+b$ や積 ab の属する類を $(a+m\mathbb{Z})+(b+m\mathbb{Z})$, $(a+m\mathbb{Z})\cdot(b+m\mathbb{Z})$ として，**本当に問題ないのだろうか**.

補題 2． 加法群 $(\mathbb{Z},+)$ に対して，$m\mathbb{Z}$ は $(\mathbb{Z},+)$ の部分群である．
$\because$ $\forall mn_1,mn_2\in m\mathbb{Z}$ に対して，$mn_1+mn_2=m(n_1+n_2)\in m\mathbb{Z}$ かつ $-(mn_1)=m(-n_1)\in m\mathbb{Z}$ となる．よって，部分群の判定条件 (第 10 回の定理 [6], p.23) より，$m\mathbb{Z}$ は $\mathbb{Z}$ の部分群.

例 3 (問題が起こる場合)． $\mathbb{Z}$ の部分群 $m\mathbb{Z}$ を用いた類別 $\mathbb{Z}/m\mathbb{Z}$ の代わりに，
3 次対称群 $S_3=\{(1),(1\,2),(1\,3),(2\,3),(1\,2\,3),(1\,3\,2)\}$ の部分群 $H=\{(1),(1\,2)\}$ を用いた類別

$$\begin{aligned}S_3&=(1)H\cup(1\,3)H\cup(2\,3)H\\&=\{(1),(1\,2)\}\cup\{(1\,3),(1\,2\,3)\}\cup\{(2\,3),(1\,3\,2)\}\\&=(1\,2)H\cup(1\,2\,3)H\cup(1\,3\,2)H\end{aligned}$$

を考えてみる．このとき，3 つの元からなる集合 $S_3/\sim=\{(1)H,(1\,3)H,(2\,3)H\}$ に対して，積 $*$ を

$$(aH)*(bH):=(a\circ b)H$$

と定義する．すなわち，代表元 a,b の積 $a\circ b=c$ の属する cH を積 $(aH)*(bH)$ として定める．しかし，これでは**積は (うまく) 定義されていない**．なぜなら,

$$(1\,3)H*(2\,3)H=(1\,3)(2\,3)H=(1\,3\,2)H=(2\,3)H$$

であるが，別の代表元を取れば,

$$(1\,3)H*(2\,3)H=(1\,2\,3)H*(2\,3)H=(1\,2\,3)(2\,3)H=(1\,2)H=(1)H$$

となり，**積 $(1\,3)H*(2\,3)H$ の結果が，代表元の選び方によって変わってしまう**からである.

• そこで，代表元の取り方にはよらずに，加法 $(a+m\mathbb{Z})+(b+m\mathbb{Z})$ と乗法 $(a+m\mathbb{Z})\cdot(b+m\mathbb{Z})$ が **well-defined である (うまく定義されている)** ことを示さないといけない．つまり，

$(a+m\mathbb{Z})=(a'+m\mathbb{Z})$ かつ $(b+m\mathbb{Z})=(b'+m\mathbb{Z})$　　$[a]=[a']$ かつ $[b]=[b']$　　$\overline{a}=\overline{a'}$ かつ $\overline{b}=\overline{b'}$

なる場合に，代表元のとり方によらず，加法と乗法の演算結果が一致すること：

$$\begin{array}{ccc} (a+b)+m\mathbb{Z}=(a'+b')+m\mathbb{Z} & [a+b]=[a'+b'] & \overline{a+b}=\overline{a'+b'} \\ ab+m\mathbb{Z}=(a'\cdot b')+m\mathbb{Z} & [ab]=[a'b'] & \overline{ab}=\overline{a'b'} \end{array}$$

を示す必要がある．($\leftarrow$ これが成立して，和 $(+)$ と積 $(\cdot)$ が **(うまく) 定義された**と言える)

定理 4． 集合 $\mathbb{Z}/m\mathbb{Z}=\{[a]\,|\,a\in\mathbb{Z}\}$ に定義された，加法 $[a]+[b]:=[a+b]$ と乗法 $[a]\cdot[b]:=[a\cdot b]$ は **well-defined である** (= うまく定義されている). ($\leftarrow$ well-defined については教科書 p.49 参照) すなわち，$[a]=[a']$ かつ $[b]=[b']$ ならば $[a+b]=[a'+b']$ 及び $[ab]=[a'b']$ が成り立つ．

$\because$ $[a]=[a']$ かつ $[b]=[b']$ より，命題 [1] から $-a+a'\in m\mathbb{Z}$, $-b+b'\in m\mathbb{Z}$ を得る．よって，補題より，$(-a+a')+(-b+b')=-(a+b)+(a'+b')\in m\mathbb{Z}$ かつ $-ab+a'b'=(-ab+a'b)+(-a'b+a'b')=(-a+a')b+(-b+b')a'\in m\mathbb{Z}$. 再び，命題 [1] より，$[a+b]=[a'+b']$ かつ $[ab]=[a'b']$ を得る．

• 類に対する演算を**代表元を用いて定めた場合，演算が well-defined であることが確認され，はじめて，演算が定義された集合** (今の場合は，$(\mathbb{Z}/m\mathbb{Z},+)$ と $(\mathbb{Z}/m\mathbb{Z},\cdot)$) **を考えることができる**．

定理 5． $(\mathbb{Z}/m\mathbb{Z},+)$ は位数 m の巡回群である．

$\because$ 演算が well-defined は確認されたので，後は群の定義 (G1), (G2), (G3) を満たすことを示す．
(G1) 結合律 整数 $a,b,c\in\mathbb{Z}$ に対する結合律 $(a+b)+c=a+(b+c)$ を用れば，$\forall[a],[b],[c]\in\mathbb{Z}/m\mathbb{Z}$ に対して，$([a]+[b])+[c]=[a+b]+[c]=[(a+b)+c]=[a+(b+c)]=[a]+[b+c]=[a]+([b]+[c])$ が成り立つ，
(G2) 単位元 (ゼロ元) は $[0]$ であり，$[a]+[0]=[a+0]=[a]=[0+a]=[0]+[a]$ $(\forall a\in\mathbb{Z})$,
(G3) $\forall[a]$ に対する**逆元**は $[-a]$ であり，$[a]+[-a]=[a+(-a)]=[0]=[(-a)+a]=[-a]+[a]$.
加法 $+$ の可換性も，$[a]+[b]=[a+b]=[b+a]=[b]+[a]$ $(\forall a\in\mathbb{Z})$ から OK.
また巡回群であることは，$\langle[1]\rangle=\{a\cdot[1]\,|\,a\in\mathbb{Z}\}=\{[1\cdot a]\,|\,a\in\mathbb{Z}\}=\{[a]\,|\,a\in\mathbb{Z}\}$ として分かる．

命題 6． $(\mathbb{Z}/m\mathbb{Z},\cdot)$ に対し，元 $[a]\in\mathbb{Z}/m\mathbb{Z}$ の逆元 $[a]^{-1}\in\mathbb{Z}/m\mathbb{Z}$ が存在 $\iff$ $\gcd(a,m)=1$.

$\because$ 互いに素な整数の特徴付け (第 11 回の定理 [7], p.30) から，
$\gcd(a,m)=1\iff\exists s,t\in\mathbb{Z}$ s.t. $as+mt=1$ であることに注意する．
($\Longrightarrow$) $[a]$ の逆元 $[b]=[a]^{-1}$ が存在するとすれば，$[a]\cdot[b]=[ab]=[1]$ であり，命題 [1] より，$-ab+1\in m\mathbb{Z}$. よって，$\exists n\in\mathbb{Z}$ s.t. $mn+ab=1$ より $\gcd(a,m)=1$ を得る．
($\Longleftarrow$) $\gcd(a,m)=1\Longrightarrow\exists n,b\in\mathbb{Z}$ s.t. $mn+ab=1$. このとき，$[a][b]=[ab]=[1]=[ba]=[b][a]$ となり，$[a]$ の逆元 $[b]=:[a]^{-1}$ が存在する．

定義 (既約剰余類，オイラー関数)． $\mathbb{Z}/m\mathbb{Z}$ の元 $a+m\mathbb{Z}$ のうち，$\gcd(a,m)=1$ となるものを**既約剰余類**という．既約剰余類全体のなす集合を $(\mathbb{Z}/m\mathbb{Z})^\times:=\{[a]\in\mathbb{Z}/m\mathbb{Z}\,|\,\gcd(a,m)=1\}$ で表す．$(\mathbb{Z}/m\mathbb{Z})^\times$ の位数を $\varphi(m)$ と表し，φ を**オイラー関数** (Euler function) と呼ぶ．

定理 7． $(\mathbb{Z}/m\mathbb{Z})^\times:=\{[a]\in\mathbb{Z}/m\mathbb{Z}\,|\,\gcd(a,m)=1\}$ に対して，$((\mathbb{Z}/m\mathbb{Z})^\times,\cdot)$ は位数 $\varphi(m)$ の可換群をなす．群 $((\mathbb{Z}/m\mathbb{Z})^\times,\cdot)$ を**既約剰余類群**という．

$\because$ 演算が well-defined は確認されたので，後は群の定義 (G1), (G2), (G3) を満たすことを示す．
(G1) 結合律 整数 $a,b,c\in\mathbb{Z}$ に対する結合律 $(ab)c=a(bc)$ を用れば，$\forall[a],[b],[c]\in(\mathbb{Z}/m\mathbb{Z})^\times$ に対して，$([a]\cdot[b])[c]=[ab]\cdot[c]=[(ab)c]=[a(bc)]=[a]\cdot[bc]=[a]([b]\cdot[c])$ が成り立つ，
(G2) 単位元は $[1]$ であり，$[a][1]=[a\cdot1]=[a]=[1\cdot a]=[1][a]$ $(\forall[a]\in(\mathbb{Z}/m\mathbb{Z})^\times)$,
(G3) 命題 6 より，$\forall[a]\in(\mathbb{Z}/m\mathbb{Z})^\times$ の**逆元** $[a]^{-1}\in\mathbb{Z}/m\mathbb{Z}$ が存在し，$[a]^{-1}$ の逆元も $[a]$ として存在するから，$[a]^{-1}\in(\mathbb{Z}/m\mathbb{Z})^\times$ である．また，可換性は $[a][b]=[ab]=[ba]=[b][a]$ より OK.

系 (有限体)． p を素数とする．$((\mathbb{Z}/p\mathbb{Z})^\times, \cdot) = \{[1], [2], \ldots, [p-1]\}$ は位数 $p-1$ の可換群である．特に，$(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ は位数 p の体 (有限体) であり，$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ とかく．(← 体については p.22)

方程式の解は四則演算が可能な体 K 上で考える事ができる (第10回, p.23参照)．有限体 $K = \mathbb{F}_p$ 上の場合，$ax + b = 0$, $x^2 = a$ を解くとは，それぞれ $ax + b \equiv 0 \pmod{p}$, $x^2 \equiv a \pmod{p}$ の解 $x \in \mathbb{F}_p$ を求めることを意味する．(← もちろん，解が存在しない場合もある)

- 次のフェルマーの定理は，**フェルマーの最終定理と間違わないよう**，小定理と呼ばれている．

定理 (フェルマーの小定理)． 素数 p と $\gcd(a, p) = 1$ なる整数 $a \in \mathbb{Z}$ に対して，

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

∵ $(\mathbb{Z}/p\mathbb{Z})^\times$ は位数 $p-1$ の可換群である．よって，$\forall [a] \in (\mathbb{Z}/p\mathbb{Z})^\times$ に対して，$\{[1], [2], \ldots, [p-1]\} = \{[a][1], [a][2], \ldots, [a][p-1]\}$ が成り立つ．全ての元の積を考えれば，積の可換性から $[1] \cdots [p-1] = [a]^{p-1}([1] \cdots [p-1])$ となる．$([1] \cdots [p-1])^{-1}$ を両辺に右からかけて，$[a]^{p-1} = [1]$ を得る．

$(\mathbb{Z}/p\mathbb{Z})^\times$ に対するフェルマーの小定理を，$(\mathbb{Z}/m\mathbb{Z})^\times$ に対して拡張するとオイラーの定理となる：

定理 (オイラーの定理)． 整数 $m \geq 2$ と $\gcd(a, m) = 1$ なる整数 $a \in \mathbb{Z}$ に対して，

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

∵ 略．(← フェルマーの小定理と同じようにやればよい)

演習問題 (期末テストの予想問題)

[1] オイラー関数の値 $\varphi(m)$, $(2 \leq m \leq 25)$ を計算せよ．
また，$\gcd(a, b) = 1$ のとき，$\varphi(a)$, $\varphi(b)$ と $\varphi(ab)$ にはどの様な関係があると予想できるか？

[2] 可換群 $((\mathbb{Z}/m\mathbb{Z})^\times, \cdot)$, $(2 \leq m \leq 10)$ の演算表を書け．(← ヒント：pp.36–37 の演算表)

[3] **[2]** を用いて，乗法群 $((\mathbb{Z}/m\mathbb{Z})^\times, \cdot)$ と加法群 $(\mathbb{Z}/m\mathbb{Z}, +)$ の同型

$(\mathbb{Z}/3\mathbb{Z})^\times \cong (\mathbb{Z}/4\mathbb{Z})^\times \cong (\mathbb{Z}/6\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$,
$(\mathbb{Z}/5\mathbb{Z})^\times \cong (\mathbb{Z}/10\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$,
$(\mathbb{Z}/7\mathbb{Z})^\times \cong (\mathbb{Z}/9\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z}$

を示せ．特に，これらは全て巡回群であることが分かる．
(← ヒント：演算表を用いた同型の定義；それぞれの演算表が，元の名前を変更し，順番も適当に入れ替えて全く同じ形にできるとき，同型であるといった)

さらに，$(\mathbb{Z}/8\mathbb{Z})^\times = \{[1], [3], [5], [7]\}$ は巡回群ではないことを示せ．

[4] 2^{10} を 11 で割った余りはいくつか？ (← ヒント: 直接計算**してもよい**)

[5] 3^{100} を 11 で割った余りはいくつか？
(← ヒント: 群 $(\mathbb{Z}/11\mathbb{Z})^\times = \{[1], \ldots, [10]\}$ と $a \equiv b \pmod{11} \Leftrightarrow [a] = [b]$ を考え，
$[a] = [3^{100}]$ なる $0 \leq a \leq 10$ を求める)

[6] 5^{1000} を 11 で割った余りはいくつか？

[7] $7^{20100708}$ を 11 で割った余りはいくつか？

[8] $7^{20100708}$ を 12 で割った余りはいくつか？

[9] 7^{13} を 12 で割った余りはいくつか？ (← ヒント: $7^{13} = 96889010407$ を**使ってもよい**)

全単射ではない群の準同型写像を考えてみる．

定義 [再掲](準同型写像)． 群 $(G,\circ)$ から群 $(G',*)$ への写像 $f : G \to G'$ が

$$\forall a,b \in G \text{ に対し，} f(a\circ b) = f(a) * f(b)$$

を満たすとき，f を G から G' への**準同型写像** (homomorphism) という．

定義 [再掲](群の同型)[無限群も含んだ一般の場合]． 群 G から群 G' への**全単射な準同型写像が存在**するとき，G **と** G' **は同型**といい，$G \cong G'$ と書く．また全単射な準同型写像を**同型写像**という．

注意 (群表による同型との関係)． 群 $(G,\circ)$ と群 $(G',*)$ が同型であるとは，全単射 (1 対 1 対応) があり，かつ二項演算 (積 $\circ$ と $*$) の構造が同じ (結果が対応している) という事である．特に，有限群 G に対しては，群表による同型の定義と準同型写像による同型の定義は同じ概念である．

定義 [再掲](有限群の同型)． 2 つの有限群 $(X,\circ)$ と $(X',\star)$ は，それぞれの演算表が，元の名前を変更し，順番も適当に入れ替えて全く同じ形にできるとき，**同型** (isomorphic) であるといい，$(X,\circ) \cong (X',\star)$ または $X \cong X'$ とかく．($\leftarrow$ X と X' は集合としては異なっていて構わない．X と X' の集合の位数が等しく，かつ積 $\circ$ と積 $\star$ は構造が同じ (=演算の結果が対応) という意味である)

(1) 加法群 $\mathbb{Z}/4\mathbb{Z} = \{\overline{0},\overline{1},\overline{2},\overline{3}\}$, 群 $G' = \{1, b_1, b_2, b_3\}$ に対して，$\mathbb{Z}/4\mathbb{Z}$ の全ての元を G' の単位元 1 に対応させる写像 $f : \mathbb{Z}/4\mathbb{Z} \to G'$, $\overline{a} \mapsto 1$ は準同型写像である．($\leftarrow$ 全射でも単射でもない)

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

f による対応 $\mapsto$

$\cdot$	1	1	1	1
1	1	1	1	1
1	1	1	1	1
1	1	1	1	1
1	1	1	1	1

$a \mapsto f(a)$,
$b \mapsto f(b)$　のとき
$a+b \mapsto f(a)\cdot f(b)$　つまり，
$f(a+b) = f(a)\cdot f(b)$　となっている．

(1)' 一般に，群 G の全ての元を群 G' の単位元 1 に対応させる写像 $G \to G'$, $g \mapsto 1$ は準同型写像．

(2) n 次対称群 S_n の元 σ に対し，符号 (σ が偶 (奇) 置換のとき $+1$ (-1)) を対応させる写像 $\mathrm{sgn}\colon S_n \ni \sigma \mapsto \mathrm{sgn}(\sigma) \in \{\pm 1\}$ は準同型写像．($\leftarrow$ 全射であるが，$n \geq 3$ に対して，単射でない)

$\circ$	(1)	a	b	c	d	e
(1)	(1)	a	b	c	d	e
a	a	b	(1)	d	e	c
b	b	(1)	a	e	c	d
c	c	e	d	(1)	b	a
d	d	c	e	a	(1)	b
e	e	d	c	b	a	(1)

sgn による対応 $\mapsto$

$\cdot$	1	-1	-1	-1	1	1
1	1	-1	-1	-1	1	1
-1	-1	1	1	1	-1	-1
-1	-1	1	1	1	-1	-1
-1	-1	1	1	1	-1	-1
1	1	-1	-1	-1	1	1
1	1	-1	-1	-1	1	1

(3) $g : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, $\overline{0} \mapsto \overline{0}$, $\overline{1} \mapsto \overline{1}$, $\overline{2} \mapsto \overline{0}$, $\overline{3} \mapsto \overline{1}$ は加法群の準同型写像．($\leftarrow$ 全射，単射でない)

(4) $h : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$, $\overline{0} \mapsto \overline{0}$, $\overline{1} \mapsto \overline{2}$ は加法群の準同型写像．($\leftarrow$ 単射であるが，全射ではない)

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

g による対応 $\mapsto$

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

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

h による対応 $\mapsto$

$+$	$\overline{0}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{2}$
$\overline{2}$	$\overline{2}$	$\overline{0}$

パスカルの三角形の色塗り (第 5 回) で (パソコンで) 見た，法 4 の世界を目を細めて見ると，法 2 の世界に見えるという現象は，準同型写像 g のことに他ならない！

群論で学ぶことを少しのぞいてみる (このページは試験範囲外)．

• $\mathbb{Z}/m\mathbb{Z}$ を，より一般の群 G とその部分群 H に拡張し，G/H を定義する．

定義 (剰余類)． H を群 G の部分群とする．
$a \in G$ に対し，$aH := \{ah \mid h \in H\}$ を H **を法とする** a **の左剰余類**という．
($\leftarrow$ G が加法群の場合には，$a + H = \{a + h \mid h \in H\}$ で，$a + m\mathbb{Z}$ はこの特別な場合になっている)

• なぜ左剰余類か？一般に群 G は非可換であり，$aH \neq Ha$ なる場合もある．よって，**左剰余類** aH **と右剰余類** Ha **を区別する**．ただし，G が可換群 (加法群) の場合には，$aH = Ha$ であり，単に**剰余類**とよぶ．

命題． 群 G の部分群 H と $a \in G$ に対して，次の (1)〜(5) は同値である：
(1) $aH = bH$ (2) $a^{-1}b \in H$ (3) $b \in aH$ (4) $a \in bH$ (5) $aH \cap bH \neq \emptyset$,
($\leftarrow$ G が加法群の場合には，以下となり，$\mathbb{Z}/m\mathbb{Z}$ の場合は命題 [1] で示した：
(1) $a + H = b + H$ (2) $-a + b \in H$ (3) $b \in a + H$ (4) $a \in b + H$ (5) $(a + H) \cap (b + H) \neq \emptyset$)

定義 (H を法として合同)． H を群 G の部分群とする．$a, b \in G$ に対し，$aH = bH$($\leftarrow$ 前命題より，$a^{-1}b \in H$ と同値) となるとき，a と b は H **を法として左合同**といい，$a \sim_l b$ とかく．($a \sim_l b$ は同値関係となる)

定義 (剰余類の集合 G/H)． G の H による (左) 剰余類の集合 $\{aH \mid a \in G\}$ を G/H とかき，($\leftarrow$ $\sim_l$ による商集合 $X/\sim_l$ のこと) 右剰余類の集合 $\{Ha \mid a \in G\}$ を $H\backslash G$ とかく．
($\leftarrow$ G が加法群の場合には，$G/H = \{a + H \mid a \in G\} = H\backslash G$)

定義 (G における H の指数)． G/H の濃度 (位数) を $|G : H|$ とかいて，G における H の**指数**という．

定理 (ラグランジュ (Lagrange) の定理)． 有限群 G とその部分群 H に対し，$|G| = |G : H||H|$

$\because$ G の H による左剰余類の集合 $G/H = \{H, a_2H, \ldots, a_kH\}$ を考える．ここで，$b \in H$ に対して，$H = \{c_1, \ldots, c_m\} \ni c_i \mapsto bc_i \in bH = \{bc_1, \ldots, bc_m\} \subset H$ は単射 ($c_i \neq c_j \Rightarrow bc_i \neq bc_j$) であり，$|H| = |bH| = m$ $(\forall b \in H)$. $G = H \cup \cdots \cup a_kH$ で各剰余類が m 個の元から成るので，$|G| = km = |G : H||H|$.

系 1． 有限群 G の部分群 H の位数 $\#H = |H|$ は，$\#G = |G|$ の約数である．

系 2． 位数 n の有限群 G の元 a に対して，$\mathrm{ord}(a) \mid \#G$．特に，$\forall a \in G$ に対して，$a^n = 1$.

系 3． 位数が素数 p の有限群は巡回群である．

命題． H は群 G の部分群とする．$aH = bH \Leftrightarrow (ca)H = (cb)H$, $Ha = Hb \Leftrightarrow H(ac) = H(bc)$, $(\forall a, b, c \in G)$. また，次の (1)〜(4) は同値である：
(1) $\forall g \in G$ に対し，$gH = Hg$;
(2) $\forall a, b, a', b' \in G$ に対し，$aH = a'H$ かつ $bH = b'H \Rightarrow (ab)H = (a'b')H$;
(3) $\forall g \in G$ に対し，$gHg^{-1} \subset H$;
(4) $\forall g \in G$ に対し，$gHg^{-1} = H$.

定義 (正規部分群)． 群 G の部分群 H が，$gH = Hg$ $(\forall g \in G)$ を満たすとき，H を G の**正規部分群** (normal subgroup) といい，$H \lhd G$ とかく．このとき，(左，右剰余類は一致するので) gH を単に**剰余類**という．

定理． H を G の正規部分群 ($H \lhd G$) とする．剰余類の集合 $G/H = \{gH \mid g \in G\}$ に対して，積 $*$ を

$$(g_1H) * (g_2H) = (g_1g_2)H$$

と定義すれば，**well-defined であり**，この演算で $(G/H, *)$ **は群をなす**．
群 G/H の単位元は H $(= eH)$，gH の逆元は $(gH)^{-1} = g^{-1}H$ である．
($\leftarrow$ G が加法群の場合には，単位元は H $(= 0 + H)$，$g + H$ の逆元は $-g + H$)

注意． 上記命題の (2) から well-defined が分かる，逆に言えば，**左剰余類と右剰余類が一致しない (正規部分群でない) 場合には，積** $*$ **は well-defined ではない**．例 2 (p.37) 参照)

定義 (剰余群，商群)． 群 $(G/H, *)$ を群 G の正規部分群 H による**剰余群**または**商群**という．